(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 748**

(51) Int. CI.:

G06F 21/30 (2013.01)
G06F 9/44 (2008.01)
G06F 3/00 (2006.01)
G06Q 30/02 (2012.01)
G06Q 50/10 (2012.01)
G06F 21/34 (2013.01)
H04L 29/06 (2006.01)
G06F 9/455 (2008.01)
G06F 21/10 (2013.01)
G06F 21/35 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.02.2013 E 17174182 (0)**

(97) Fecha y número de publicación de la concesión europea: **15.08.2018 EP 3239878**

(54) Título: **Activación de contenido por medio de autenticación basada en interacciones, sistemas y método**

(30) Prioridad:

24.02.2012 US 201261603049 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.10.2018

(73) Titular/es:

NANT HOLDINGS IP LLC (100.0%)
9920 Jefferson Boulevard
Culver City, CA 90232, US

(72) Inventor/es:

SOON-SHIONG, PATRICK

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Activación de contenido por medio de autenticación basada en interacciones, sistemas y método

La presente solicitud reivindica prioridad con respecto a la solicitud provisional de Estados Unidos con número de serie 61/603049, presentada el 24 de febrero de 2012.

Campo de la invención

El campo de la invención es las tecnologías de distribución de contenido.

Antecedentes

La siguiente descripción incluye información que puede resultar útil para entender la presente invención. No constituye un reconocimiento de que alguna de la información proporcionada en este documento sea técnica anterior o relevante para la invención reivindicada en la presente, o de que cualquier publicación a la que se haga referencia de manera específica o implícita sea técnica anterior.

La cantidad de contenido que se distribuye a través de redes hacia dispositivos electrónicos continúa creciendo a una velocidad alarmante, impulsada por consumidores de contenido que buscan satisfacer su necesidad insaciable de contenido. Desafortunadamente, los consumidores de contenido no están siempre autorizados a acceder al contenido que desean. Además, normalmente los proveedores de contenido carecen de control sobre la distribución de contenido de una manera tal que garantice que los derechos del proveedor quedan protegidos. El conflicto entre la demanda del contenido y los derechos del mismo genera frustración de los consumidores y los proveedores. Se requiere una infraestructura que permita una presencia permanente del contenido, aunque permitiendo solamente que el mismo se distribuya a individuos tras una autenticación válida. Y lo que es más interesante, todavía debe apreciarse la posibilidad de uso de los objetos cotidianos, u objetos en relación mutua, como llave para activar contenido de una manera controlada que proteja derechos de los proveedores de contenido y satisfaga la demanda, por parte de los consumidores, de una gratificación inmediata de contenido. Aún adicionalmente, todavía debe apreciarse la posibilidad de uso de objetos cotidianos para obtener acceso a niveles diferentes de contenido, lo cual podría dar origen a interacciones más dinámicas con objetos.

Parte del esfuerzo ha ido dirigido a enlazar marcas con formas sociales de televisión. Por ejemplo, Second Screen Networks™ (véase el URL www.secondscreen.com) permite que proveedores de contenido envíen anuncios a una segunda pantalla de un usuario (por ejemplo, un teléfono celular) cuando se presenta contenido correspondiente en la televisión. No obstante, un planteamiento de este tipo no consigue afrontar la demanda de contenido, por parte de un consumidor, en cualquier instante de tiempo y sin ningún televisor cerca. Además, el planteamiento de Second Screen requiere que el consumidor opte por entrar en el sistema, más que ofrecer acceso a una capa ubicua de contenido con presencia permanente.

Esfuerzos adicionales se han dirigido al uso de técnicas de reconocimiento biométricas como base para establecer la identidad de una persona como parte de sistemas de autenticación. Por ejemplo, la memoria descriptiva de la solicitud de patente europea EP 2 348 458, de Murakami et al., titulada “Biometric Authentication System”, presentada el 3 de septiembre de 2010, describe el uso de características biométricas para determinar la identidad de un usuario basándose en una autenticación biométrica. Además, la publicación de solicitud de patente de Estados Unidos 2011/0311112, de Matsuyama et al., titulada “Identification Device, Identification Method, and Storage Medium”, presentada el 16 de junio de 2011, da a conocer la identificación de una persona sobre la base de datos de características extraídos a partir de cuadros de imagen de la cara de la persona. Cuando no se han identificado datos de características específicos en tramas sucesivas, los datos de características se asocian al área de la cara de las tramas sucesivas. Todavía adicionalmente, la patente de Estados Unidos 8.194.938, de Wechsler et al., titulada “Face Authentication Using Recognition-by-Parts, Boosting, and Transduction”, presentada el 1 de junio de 2010, describe la autenticación de la cara de una persona mediante la comparación de “parches” de imágenes capturadas de la cara de la persona con parches conocidos, donde los parches se pueden extraer por medio de SIFT u ondículas de Gabor. Y lo que es más interesante, cada una de las técnicas dadas a conocer requiere una interpretación a priori de las características biométricas, y no resulta adecuada para su uso con respecto a clases de objetos sin restricciones.

No obstante, hay técnicas disponibles que ofrecen al menos una vía de avance mínima con respecto a la identificación o reconocimiento de clases diferentes de objetos más allá de simplemente identificar clases conocidas a priori de características biométricas. Por ejemplo, el resumen de la patente japonesa correspondiente a la referencia JP4164737, de Yokono, titulada “Object Recognition Device, Object Recognition Method, and Robot Equipment” (inglés), presentada el 24 de mayo de 2002, describe un sistema de aprendizaje para robots, donde un robot aprende a reconocer un objeto desconocido colocando el objeto desconocido en una posición predeterminada con respecto al aparato de formación de imágenes. Adicionalmente, el resumen de la patente japonesa correspondiente a la referencia JP2005202653, de Matsugi et al., titulada “Behavior Recognition Device and Method, Animal Object Recognition Device and Method, Equipment Control Device and Method, and Program” (inglés), presentada el 15 de enero de 2004, describe el reconocimiento de objetos sobre la base de características

primitivas. Las características primitivas se pueden observar durante un periodo de tiempo con el fin de generar una categoría de comportamiento de salida.

El reconocimiento basado en imágenes incluye la patente de Estados Unidos 7016532 de propiedad conjunta, titulada “Image Capture and Identification System and Process”, presentada el 5 de septiembre de 2001; la patente de Estados Unidos 7680324, titulada “Use of Image-Derived Information as Search Criteria for Internet and other Search Engines”, presentada el 15 de agosto de 2005; la patente de Estados Unidos 7565008, titulada “Data Capture and Identification System and Process”, presentada el 26 de enero de 2006; y la patente de Estados Unidos 7477780, titulada “Data Capture and Identification System and Process”, presentada el 22 de marzo de 2004, todas ellas a nombre de Boncyk et al. Boncyk describe el cálculo de parámetros relevantes a partir de datos de imagen de un objeto, y a continuación el uso de los parámetros para buscar imágenes de objetos conocidos en una base de datos.

Las referencias anteriores, al menos en cierto nivel, permiten el reconocimiento o la identificación de objetos, aunque no consiguen hacer frente a la autenticación de un usuario o a la autorización de acceso a contenido de acuerdo con diferentes niveles de acceso, sobre la base de diferentes formas de captura de datos.

Otros trabajos han ido dirigido al uso de diferentes técnicas de captura de datos para autenticar usuarios. Por ejemplo, la patente de Estados Unidos 6.687.390, de Avni et al., titulada “System for and Method of Web Signature Recognition System Based on Object Map”, presentada el 4 de diciembre de 2001, da a conocer la validación de una identidad de un usuario basándose en cómo el usuario mueve un dispositivo señalador en un ordenador, para manipular un cursor sobre una imagen gráfica de fondo.

Todavía adicionalmente, se han dirigido trabajos a la autenticación de objetos físicos calificándolos como no falsificaciones. La patente de Estados Unidos 5.974.150, de Kaish et al., titulada “System and Method for Authentication of Goods”, presentada el 6 de julio de 1998, describe el uso de la posición de una pluralidad de elementos (por ejemplo, fibras diacrónicas) dispuestos en un patrón irregular en un soporte (por ejemplo, papel) para autenticar productos como verdaderos por contraposición a las falsificaciones. En un estilo similar a Kaish, la patente de Estados Unidos 7.995.196, de Fraser, titulada “Authentication Method and System”, presentada el 21 de abril de 2009, intenta también proporcionar técnicas para autenticar objetos basándose en un patrón de dispersión física de un conjunto de elementos (por ejemplo, fibras) sobre un sustrato. La patente de Estados Unidos 8.245.922, de Gerigk et al., titulada “Method and Device for Identifying and Authenticating Objects”, presentada el 19 de noviembre de 2010, describe también la autenticación de objetos. Gerigk describe la codificación de un objeto con un código en una región de código, que dispersa radiación electromagnética. Aunque estas referencias aportan utilidad con respecto a la autenticación *per se*, no consiguen apreciar que el contenido podría disponer de diferentes niveles de acceso.

Uno de los ejemplos de técnica para proporcionar acceso a contenido incluye la patente de Estados Unidos 7.283.973, de Loghmani et al., titulada “Multi-Modal Voice-Enable Content Access and Delivery System”, presentada el 29 de octubre de 2002. Loghmani describe el uso de reconocimiento de voz o tonos de DTMF para permitir que un usuario acceda a contenido a través de un teléfono. En la patente de Estados Unidos 7.380.280, de Jong, titulada “Rights Locker for Digital Content Access Control”, presentada el 15 de octubre de 2003, se describe un avance adicional hacia la concesión de autorización para acceder a contenido. De Jong sugiere el uso de un planteamiento de un sistema de gestión de tokens para limitar el acceso a contenido. Todavía adicionalmente, la patente de Estados Unidos 7.953.079, de John et al., titulada “Method and Apparatus to Control Access to Content”, presentada el 4 de junio de 2007, describe la provisión de acceso a contenido sobre la base de una política de acceso a contenido, en la que el contenido se clasifica por tipo, posiblemente a través del uso de herramientas de reconocimiento de voz, reconocimiento de texto o de imágenes. Todavía adicionalmente, la publicación de solicitud de patente de Estados Unidos de Roberts et al., titulada “Methods and Systems for Controlling Presentation of Media Content Based on User Interaction”, presentada el 30 de junio de 2009, describe la monitorización de un usuario para determinar si el mismo está interaccionando de manera activa o pasiva con contenido de medios. Se presenta el contenido al usuario basándose en los perfiles de una interacción.

Las referencias descritas anteriormente hasta el momento no consiguen proporcionar un aumento de la seguridad mediante la posibilidad de que un usuario utilice un objeto como clave de autorización. No obstante, el resumen de la solicitud internacional WO 2012/085378, de Fondeur et al., titulada “Method for Enabling Authentication of Identification, and Related Verification Systems”, presentada el 29 de noviembre de 2011, describe la captura de una imagen de un objeto que es seleccionado en secreto por una persona, donde la imagen del objeto se usa para registrar la persona en un sistema. Fondeur contempla simplemente el uso de una imagen de un objeto para el registro del usuario, y no prevé el uso de diferentes modalidades para la autorización. No obstante, la solicitud de patente de Estados Unidos 2011/0161232, de Brown, titulada “Virtualization of Authentication Token for Secure Applications”, presentada del 28 de diciembre de 2009, realiza todavía un progreso adicional. Brown describe la captación de imágenes de claves físicas (por ejemplo, llaves de coche, llaves de la casa, etcétera), u otros tokens físicos, como partes de un tipo de autenticación de “lo que tienes”. Brown describe que las imágenes de los tokens físicos se pueden combinar con una huella vocal, un factor de autenticación de “lo que tienes”, para crear un protocolo de autenticación multi-factor más resistente. Desafortunadamente, el sistema de Brown simplemente describe de manera sencilla el uso de múltiples claves sin tener en cuenta la disposición relativa.

En algunas realizaciones, los números que expresan cantidades de ingredientes, propiedades, tales como concentración, condiciones de reacción, y otros, usados para describir y reivindicar ciertas realizaciones de la invención, deben interpretarse como modificados, en algunos casos, por el término “aproximadamente”. Por consiguiente, en algunas realizaciones, los parámetros numéricos que se exponen en la descripción redactada y las reivindicaciones adjuntas, son aproximaciones que pueden variar en función de las propiedades deseadas cuya obtención es pretendida por una realización particular. En algunas realizaciones, los parámetros numéricos deben considerarse teniendo en cuenta el número de dígitos significativos expuestos y aplicando técnicas de redondeo comunes. A pesar de que los intervalos y parámetros numéricos que exponen el alcance genérico de algunas realizaciones de la invención son aproximaciones, los valores numéricos expuestos en los ejemplos específicos se aportan con la mayor precisión que resulta viable. Los valores numéricos presentados en algunas realizaciones de la invención pueden contener ciertos errores que son un resultado necesario de la desviación estándar que se observa en sus mediciones de prueba respectivos.

Tal como se usan en la descripción de la presente y en todas las reivindicaciones que se ofrecen a continuación, el significado de “un”, “una” y “el/la/los/las” incluye una referencia diversa plural a no ser que el contexto dictamine claramente lo contrario. Además, tal como se usa en la descripción de la presente, el significado de “en” incluye “en” y “sobre” a no ser que el contexto dictamine claramente lo contrario.

La mención de intervalos de valores en la presente está destinada simplemente a servir como método abreviado para referirse individualmente a cada valor independiente que se sitúa dentro del intervalo. A no ser que se indique lo contrario en el presente documento, cada valor individual se incorpora en la memoria descriptiva como si se mencionase individualmente en la presente. Todos los métodos descritos en el presente documento se pueden llevar a cabo en cualquier orden adecuado, a no ser que se indique lo contrario en la presente, o el contexto se oponga claramente. El uso de todos y cada uno de los ejemplos, o de lenguaje ilustrativo (por ejemplo, “tal como”) aportado con respecto a ciertas realizaciones en la presente, está destinado meramente a clarificar mejor la invención, y no impone ninguna limitación sobre el alcance de la invención reivindicada de otra manera. Nada del lenguaje de la memoria descriptiva debe considerarse como indicativo de ningún elemento no reivindicado, esencial para la práctica de la invención.

Los grupos de elementos alternativos o realizaciones de la invención que se dan a conocer en la presente, no deben considerarse como limitaciones. A cada miembro de un grupo se le puede hacer referencia y el mismo se puede reivindicar individualmente o en cualquier combinación con otros miembros del grupo u otros elementos que se encuentran en la presente. Uno o más miembros de un grupo se pueden incluir en un grupo, o eliminar del mismo, por motivos de conveniencia y/o patentabilidad. Cuando se produzca cualquiera de estas inclusiones o eliminaciones, se considera que la memoria descriptiva en la presente contiene el grupo según se modifique, dando así satisfacción a la descripción redactada de todos los grupos de Markush usados en las reivindicaciones adjuntas.

Un sistema más ideal proporcionaría la autenticación o autorización de una entidad para acceder a diversos niveles de contenido sobre la base de una yuxtaposición de los objetos, uno con respecto a otro, en lugar de la mera existencia de un objeto como token de seguridad. Un planteamiento de este tipo, según se describe posteriormente en el trabajo del solicitante, resulta ventajoso al ofrecer una capacidad de negación plausible, un acceso o control detallado, u otras características de nivel de acceso, al mismo tiempo que permitiendo que un proveedor de contenido mantenga el control sobre su contenido.

Así, sigue existiendo una necesidad de sistemas y métodos de autenticación y activación de contenido.

Sumario de la invención

La materia objeto de la invención proporciona aparatos, sistemas y métodos en los cuales se puede activar contenido basándose en el reconocimiento de que objetos reales en un entorno o escena se pueden considerar objetos de autenticación con respecto a la obtención de acceso al contenido.

Un aspecto de la materia objeto de la invención incluye un método de activación de contenido de realidad aumentada (AR). El método comprende permitir que un dispositivo electrónico acceda a un agente de autenticación; obtener, por parte del dispositivo electrónico, una representación digital de una interacción con un entorno físico que comprende una pluralidad de objetos; discriminar por lo menos dos objetos diferentes de entre la pluralidad de objetos, como primer objeto de autenticación válido y segundo objeto de autenticación válido sobre la base de la representación digital; y obtener un primer conjunto de características de autenticación asociadas al primer objeto de autenticación válido y un segundo conjunto de características de autenticación asociadas al segundo objeto de autenticación válido a partir de la representación digital. El método se caracteriza por que comprende además: establecer, por parte del agente de autenticación, un nivel de acceso a contenido relacionado con el contenido de AR en función de una yuxtaposición del primer conjunto de características de autenticación con respecto al segundo conjunto de características de autenticación, en donde la yuxtaposición se basa en al menos información de tiempo relativo; activar, por parte del agente de autenticación, el contenido de AR basándose en el nivel de acceso al contenido y en una o más interacciones en el mundo real; y configurar un dispositivo de salida para que presente el contenido de AR de acuerdo con el nivel de acceso al contenido.

A continuación se aportan realizaciones del método. Por lo menos uno del primer objeto de autenticación válido y del segundo objeto de autenticación válido puede comprender un objeto de AR u otro tipo de objeto virtual. El contenido de AR puede comprender un juego. El nivel de acceso al contenido puede representar un grado o alcance hasta el cual puede interaccionar un usuario con el juego. Diferentes yuxtaposiciones del primer conjunto de características de autenticación con respecto al segundo conjunto de características de autenticación pueden determinar o permitir diferentes niveles de acceso al juego. La interacción o interacciones en el mundo real pueden incluir una interacción con una ubicación específica en el mundo real. La interacción o interacciones en el mundo real pueden incluir una o más interacciones con otros usuarios del contenido de AR. Diferentes yuxtaposiciones del primer conjunto de características de autenticación con respecto al segundo conjunto de características de autenticación pueden permitir diferentes niveles de control sobre el contenido de AR, incluyendo uno o más de autorizar a un usuario a: desplazar en el tiempo el contenido de AR, iniciar o participar en una transacción relacionada con el contenido de AR, copiar o grabar el contenido de AR, editar el contenido de AR, compartir el contenido de AR, e interaccionar de manera directa o indirecta con el contenido de AR. El contenido de AR puede comprender una promoción asociada a un producto, incluyendo uno o más de un cupón, un mensaje publicitario, una oferta, una rebaja, un número de lotería y un anuncio. La promoción puede estar asociada a por lo menos uno del primer objeto de autenticación válido y el segundo objeto de autenticación válido. El contenido de AR puede comprender por lo menos uno de una aplicación o módulo de software, datos de imagen, datos de vídeo, datos de audio, un historial médico, datos de juego, datos promocionales, información de bienes o servicios, una orden, una instrucción, y una instrucción u orden robótica. El contenido de AR puede comprender por lo menos dos modalidades diferentes, incluyendo por lo menos una de una modalidad auditiva, visual, cinestésica, gestual, olfativa, táctil, gustativa, y sensorial. El contenido de AR puede comprender por lo menos una de las siguientes: información de transacciones, información de entretenimiento, información de noticias, información deportiva, información promocional, información médica, información de seguridad e información de juegos. El método puede comprender, además, obtener datos multimodales como parte de la representación digital, incluyendo por lo menos dos de los siguientes tipos de datos modales: datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración y datos de rumbo. La obtención de por lo menos uno del primer conjunto de características de autenticación y del segundo conjunto de características de autenticación puede incluir obtener por lo menos dos conjuntos de características de diferentes modalidades correspondientes a por lo menos dos diferentes de los por lo menos dos tipos de datos modales. La obtención del primer conjunto de características de autenticación puede incluir obtener características de imagen a partir de datos de imagen del primer objeto de autenticación válido en la representación digital. El primer conjunto de características de autenticación puede comprender datos de imagen de una parte del primer objeto de autenticación válido. La obtención del segundo conjunto de características de autenticación puede incluir obtener características de imagen a partir de datos de imagen del segundo objeto de autenticación válido en la representación digital. El segundo conjunto de características de autenticación puede comprender datos de imagen de una parte del segundo objeto de autenticación válido. La obtención de por lo menos uno del primer conjunto de características de autenticación y el segundo conjunto de características de autenticación puede incluir calcular un valor *hash* como característica de autenticación a partir de la representación digital. Por lo menos uno del primer conjunto de características de autenticación y del segundo conjunto de características de autenticación puede incluir por lo menos una de las siguientes: una característica de Transformada de Características Invariantes a la Escala (SIFT), un rasgo de imagen, y una profundidad de campo. Por lo menos uno del primer conjunto de características de autenticación y el segundo conjunto de características de autenticación puede incluir por lo menos dos de los siguientes tipos de datos de características: datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración y datos de rumbo. El método puede comprender, además, activar el contenido de AR en función de criterios desencadenantes de la activación. Los criterios desencadenantes de la activación pueden depender de un tiempo absoluto. Los criterios desencadenantes de la activación pueden depender de una o más solicitudes de autenticación. La configuración del dispositivo de salida para que presente el contenido de AR puede comprender dar instrucciones al dispositivo de salida para que lance una máquina virtual. El método puede comprender, además, proteger la máquina virtual con respecto a derechos de contenido de acuerdo con el nivel de acceso al contenido. El método puede comprender, además, restringir el acceso, por parte de la máquina virtual, al contenido de AR de acuerdo con el nivel de acceso al contenido. El dispositivo electrónico puede comprender por lo menos uno de los siguientes: un teléfono celular, un ordenador de tipo tableta, un ordenador, una consola de juegos, un vehículo, un quiosco interactivo, una máquina expendedora, un robot, un electrodoméstico, un dispositivo médico y un sistema de seguridad. El dispositivo electrónico puede comprender el dispositivo de salida.

Otro aspecto de la materia objeto de la invención incluye métodos de activación de contenido. Un dispositivo electrónico puede acceder a un agente de autenticación capaz de conceder acceso a contenido. En algunas realizaciones, el dispositivo electrónico obtiene una representación digital, posiblemente una representación multi-modal, de una interacción (por ejemplo, diálogo, imágenes, trabajo, reproducción, captación, monitorización, etcétera) con al menos un objeto físico para un motor de reconocimiento, que actúa posiblemente como agente de autenticación.

El método puede incluir además discriminar por lo menos dos objetos en el entorno, como objetos de autenticación válidos, basándose en la representación digital, donde los objetos de autenticación válidos se pueden discriminar

con respecto a otros objetos que no están relacionados con la autenticación. El método puede incluir además obtener conjuntos de características de autenticación relacionados con los objetos de autenticación válidos, donde las características de autenticación se pueden determinar a partir de la representación digital del objeto físico. Las características de autenticación de ejemplo pueden incluir un código *hash* calculado a partir de datos de imagen o de audio, características de Transformada de Características Invariantes a la Escala (SIFT), firmas de audio, posiciones, tiempo, u otros aspectos asociados a la representación digital. Otra etapa del método incluye establecer, posiblemente por medio del agente de autenticación, un nivel de acceso a contenido en función de una yuxtaposición de los conjuntos de características de autenticación unos con respecto a otros en un espacio de interacción, donde los atributos de la yuxtaposición se pueden usar como índice a una base de datos de nivel de contenido o de acceso. A continuación, el agente de autenticación puede activar contenido asociado al objeto físico, configurando el dispositivo electrónico para presentar o reproducir el contenido de acuerdo con el nivel de acceso a contenido.

Aún otro aspecto de la materia objeto de la invención incluye un sistema de distribución de contenido que comprende una base de datos de objetos de autenticación, una plataforma de reconocimiento y un agente de autenticación. Preferentemente, la base de datos de objetos de autenticación almacena múltiples elementos de autenticación, donde cada elemento puede representar un objeto, real o virtual, que puede ser usado por individuos como clave de autenticación. Por ejemplo, una persona podría registrar una planta de la casa como elemento de autenticación propio. Preferentemente, cada elemento de autenticación comprende una o más características de autenticación que son consideradas como características válidas por las cuales el elemento se puede utilizar para la autenticación; por ejemplo, parte frontal de un muñeco de acción de juguete con respecto a la parte posterior de un muñeco de acción de juguete. La plataforma de reconocimiento obtiene, o adquiere de otra manera, una representación digital de una escena que tiene uno o más objetos. La plataforma analiza la representación digital para identificar los objetos a través de la obtención de una o más características de objetos. La plataforma está configurada además para reconocer por lo menos uno de los objetos en la escena, como elemento de autenticación asociado al usuario basándose en una comparación de las características de los objetos con las características de autenticación del elemento. El agente de autenticación puede usar las características de autenticación presentes en la escena para obtener niveles de acceso a contenido, los cuales se pueden utilizar para autorizar contenido que se puede presentar en un dispositivo electrónico.

Todavía otro aspecto de la materia objeto de la invención incluye métodos para obtener información de productos. Los métodos pueden incluir proporcionar acceso a un servidor de reconocimiento, que actúa posiblemente como motor de búsqueda, un minorista en línea, u otro servicio. El servidor de reconocimiento puede obtener un cuadro de vídeo capturado a partir de un flujo continuo de vídeo. Por ejemplo, un individuo puede capturar una imagen fija de un programa de televisión, un anuncio, o una película, donde la imagen fija representa el cuadro de vídeo capturado. El servidor de reconocimiento se puede configurar además para obtener características asociadas al cuadro, y para identificar por lo menos un flujo continuo de vídeo de origen a partir del cual se capturó el cuadro basándose en las características. Una vez que se ha identificado el flujo continuo de vídeo, el método puede incluir además obtener información de productos asociada al flujo continuo de vídeo identificado, a partir de una base de datos de productos. La información de productos se puede presentar en un dispositivo electrónico.

Todavía otro aspecto de la materia objeto de la invención incluye un método de activación de contenido. El método puede comprender permitir que un dispositivo electrónico acceda a un agente de autenticación; obtener, por parte del dispositivo, una representación digital de una interacción con un entorno físico que comprende una pluralidad de objetos físicos; discriminar por lo menos dos objetos diferentes de entre la pluralidad de objetos físicos en el entorno, como primer objeto de autenticación válido y segundo objeto de autenticación válido sobre la base de la representación digital; obtener un primer conjunto de características de autenticación a partir de la presentación digital y asociadas al primer objeto de autenticación válido, y un segundo conjunto de características de autenticación a partir de la presentación digital y asociadas al segundo objeto de autenticación válido; establecer, por parte del agente de autenticación, un nivel de acceso a contenido en función de una yuxtaposición del primer conjunto de características de autenticación con respecto al segundo conjunto de características de autenticación; activar, por parte del agente de autenticación, contenido basándose en el nivel de acceso al contenido; y configurar un dispositivo de salida para que presente el contenido de acuerdo con el nivel de acceso al contenido.

A continuación se aportan realizaciones del método. El método puede comprender, además, obtener datos multimodales como parte de la representación digital, incluyendo por lo menos dos de los siguientes tipos de datos modales: datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración y datos de rumbo. La etapa de obtención del primer conjunto de características de autenticación puede incluir obtener por lo menos dos conjuntos de características de modalidades diferentes. La etapa de obtención del primer conjunto de características de autenticación puede incluir obtener características de imagen a partir de datos de imagen del primer objeto de autenticación válido en la representación digital. El primer conjunto de características de autenticación puede comprender datos de imagen de una parte del primer objeto de autenticación válido. La etapa de obtención de un primer conjunto de características de autenticación puede incluir calcular un valor *hash* como característica de autenticación a partir de la representación digital asociada al primer objeto de autenticación válido. El primer conjunto de características de autenticación puede incluir por lo menos una

de las siguientes: una característica de SIFT, un rasgo de imagen, y una profundidad de campo. El primer conjunto de características de autenticación puede incluir por lo menos dos de los siguientes tipos de datos de características: datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración y datos de rumbo. El método puede comprender, además, determinar la yuxtaposición del primer conjunto de características de autenticación con respecto al segundo conjunto de características de autenticación basándose en información de posición relativa obtenida a partir de posiciones relativas del primer objeto de autenticación válido con respecto al segundo objeto de autenticación válido en la representación digital. El método puede comprender, además, determinar la yuxtaposición en función de información de posición relativa obtenida a partir del primer conjunto de características de autenticación y del segundo conjunto de características de autenticación. El método puede comprender, además, determinar la yuxtaposición del primer conjunto de características de autenticación con respecto al segundo conjunto de características de autenticación basándose en información de orientación relativa obtenida a partir de orientaciones relativas del primer objeto de autenticación válido con respecto al segundo objeto de autenticación válido en la representación digital. El método puede comprender, además, determinar la yuxtaposición en función de información de orientación relativa obtenida a partir del primer conjunto de características de autenticación y del segundo conjunto de características de autenticación. Por lo menos uno del primer y del segundo objetos de autenticación válidos puede comprender soportes impresos. Los soportes impresos pueden comprender por lo menos uno de los siguientes: un permiso de conducir, un pasaporte, una firma, un cheque, un documento, un cartel, una valla publicitaria, una fotografía, una imagen representada, un libro, un periódico, y una revista. Por lo menos uno del primer y del segundo objetos de autenticación válidos puede comprender un objeto sustancialmente tridimensional. El objeto sustancialmente tridimensional puede comprender por lo menos uno de los siguientes: una persona, una cara, un animal, un vehículo, un edificio, un juguete, una planta, un dispositivo informático, una construcción, un alimento y una figurita. El primer objeto de autenticación válido puede comprender un dispositivo informático que tenga una imagen representada. El primer conjunto de características de autenticación puede comprender por lo menos tres características de autenticación. El primer conjunto de características de autenticación puede comprender por lo menos siete características de autenticación. El método puede comprender, además, presentar una promoción asociada a un producto, como contenido. El producto puede estar asociado al primer objeto de autenticación válido de la autenticación. La promoción puede comprender por lo menos uno de los siguientes: un cupón, un mensaje publicitario, una oferta, una rebaja, una lotería y un anuncio. El contenido puede comprender por lo menos una de las siguientes: información de transacciones, información de entretenimiento, información de noticias, información deportiva, información promocional, información médica, información de seguridad e información de juegos. La etapa de activar el contenido puede incluir activar el contenido en función de criterios desencadenantes de la activación. Los criterios desencadenantes de la activación pueden depender de un tiempo absoluto. Los criterios desencadenantes de la activación pueden depender de una serie de solicitudes de autenticación. Los criterios desencadenantes de la activación pueden depender de otros factores que no sean características dentro del primer y del segundo conjuntos de características de autenticación. Los criterios desencadenantes de la activación pueden depender de factores exclusivos de las características de autenticación. El primer conjunto de características de autenticación puede carecer de información obtenida a partir de una etiqueta simbólica asociada al primer objeto de autenticación válido. Las características de autenticación pueden carecer de datos de código de barras. La etapa de configurar el dispositivo de salida para presentar el contenido puede comprender dar instrucciones al dispositivo de salida para lanzar una máquina virtual. El método puede comprender, además, proteger la máquina virtual con respecto a los derechos de contenido de acuerdo con el nivel de acceso. El método puede comprender, además, restringir el acceso, por parte de la máquina virtual, a contenido de acuerdo con los niveles de acceso a contenido. El dispositivo electrónico puede comprender por lo menos uno de los siguientes: un teléfono celular, un ordenador de tipo tableta, un ordenador, una consola de juegos, un vehículo, un quiosco interactivo, una máquina expendedora, un robot, un electrodoméstico, un dispositivo médico y un sistema de seguridad. El dispositivo electrónico puede comprender el dispositivo de salida.

Diversos objetivos, características, aspectos y ventajas de la materia objeto de la invención se pondrán más claramente de manifiesto a partir de la siguiente descripción detallada de realizaciones preferidas, junto con las figuras de los dibujos adjuntos, en las cuales los números que son iguales representan los mismos componentes.

Breve descripción de los dibujos

La Fig. 1 es un esquema de un ecosistema de distribución de contenido y de autenticación transmedia multi-modal.

La Fig. 2 es un esquema de una plataforma de reconocimiento que discrimina objetos de autenticación dentro de un entorno, con respecto a otros objetos.

La Fig. 3 es una ilustración del análisis de representaciones digitales de objetos para obtener conjuntos de características de autenticación.

La Fig. 4 es una ilustración de una yuxtaposición de conjuntos de características de autenticación en un espacio de interacción.

La Fig. 5 es una ilustración de la determinación de niveles de acceso a contenido sobre la base de una yuxtaposición de conjuntos de figuras de autenticación.

La Fig. 6 es un esquema de un método para activar contenido.

Descripción detallada

Debe indicarse que, aunque la siguiente descripción se centra en sistemas de distribución de contenido o de autenticación basados en un ordenador/servidor, se consideran como adecuadas diversas configuraciones alternativas y las mismas pueden utilizar diversos dispositivos informáticos incluyendo servidores, interfaces, sistemas, bases de datos, agentes, entidades pares, motores, controladores, u otros tipos de dispositivos informáticos que funcionan de manera individual o en conjunto. Debe apreciarse que los dispositivos informáticos comprenden un procesador configurado para ejecutar instrucciones de software almacenadas en un soporte de almacenamiento legible por ordenador, no transitorio, físico (por ejemplo, una unidad de disco duro, una unidad de estado sólido, una RAM, *flash*, ROM, etcétera). Las instrucciones de software preferentemente configuran el dispositivo informático para proporcionar las funciones, responsabilidades u otras funcionalidades que se describen posteriormente con respecto al aparato dado a conocer. En realizaciones especialmente preferidas, los diversos servidores, sistemas, bases de datos o interfaces intercambian datos utilizando protocolos o algoritmos normalizados, basados posiblemente en HTTP, HTTPS, AES, intercambios de claves públicas-privadas, APIs de servicios web, protocolos conocidos de transacciones financieras, u otros métodos de intercambio de información electrónica. Los intercambios de datos se efectúan preferentemente a través de una red por conmutación de paquetes, Internet, una LAN, una WLAN, una VPN, u otro tipo de red por conmutación de paquetes.

Debe apreciarse que las técnicas dadas a conocer proporcionan muchos efectos técnicos ventajosos, incluyendo la generación de una o más señales de activación de contenido para dispositivos electrónicos. La señal de activación configura el dispositivo electrónico de manera que quede habilitado para presentar contenido activado. Por ejemplo, el dispositivo electrónico recibe la señal de activación a través de una red y, como respuesta, el dispositivo electrónico instancia una máquina virtual que está autorizada a presentar contenido a un usuario de acuerdo con los niveles de acceso a contenido.

La siguiente descripción proporciona muchas realizaciones de ejemplo de la materia objeto de la invención. Aunque cada realización representa una combinación individual de elementos inventivos, se considera que la materia objeto de la invención incluye todas las combinaciones posibles de los elementos dados a conocer. Así, si una realización comprende elementos A, B y C, y una segunda realización comprende los elementos B y D, entonces, se considera también que la materia objeto de la invención incluye otras combinaciones restantes de A, B, C o D, aún cuando no se hayan dado a conocer explícitamente.

Tal como se usa en la presente, y no ser que el contexto dictamine lo contrario, la expresión “acoplado a” está destinada a incluir tanto un acoplamiento directo (en el cual dos elementos que están acoplados entre sí están en contacto mutuo) como un acoplamiento indirecto (en el cual hay por lo menos un elemento adicional situado entre los dos elementos). Por tanto, las expresiones “acoplado a” y “acoplado con” se usan como sinónimas. En un contexto de redes como el que se describe en este documento, las expresiones “acoplado a” y “acoplado con” también pueden significar “acoplado comunicativamente con”.

Visión general

La Figura 1 ilustra un ecosistema de autenticación y de distribución de contenido. En el ejemplo mostrado, se activa contenido basándose en la autenticación de un usuario o dispositivo en función de una interacción multi-modal 105 con una escena 100. En algunas realizaciones, la interacción multi-modal 105 incluye tomar una imagen de uno o más objetos 120A ó 120B del mundo real, a partir de un dispositivo electrónico 110 (por ejemplo, un teléfono celular, un vehículo, etcétera) según se ilustra, donde el dispositivo electrónico 110 también puede funcionar como dispositivo de salida. Los dispositivos electrónicos de ejemplo incluyen un teléfono celular, un ordenador de tipo tableta, un ordenador convencional, una consola de juegos, un vehículo, un quiosco interactivo, una máquina expendedora, un robot, un electrodoméstico, un dispositivo médico, un sistema de seguridad, u otro dispositivo. Debe apreciarse que las interacciones multi-modales 105 pueden abarcar un amplio espectro de interacciones y datos multi-modales. Las interacciones de ejemplo con el entorno pueden incluir hacer deporte, caminar, ir de compras, comprar, imágenes, recogida de datos ambientales, monitorización, escuchar, jugar, trabajar, u otros tipos de interacciones. Los datos de interacción se pueden obtener a partir de uno o más sensores que capturan diferentes modalidades de datos. Las modalidades de ejemplo incluyen datos de vídeo, datos de audio, datos cinestésicos, datos de posición, datos de tiempo, datos de presión, datos de temperatura, datos de noticias, u otros tipos de datos. Los datos de sensores asociados al entorno se pueden obtener por medio de sensores en el dispositivo electrónico 110, por ejemplo un teléfono celular, (por ejemplo, acelerómetros, magnetómetros, brújulas, micrófonos, GPS, radiocomunicaciones, etcétera) o por medio de sensores en otros dispositivos distintos o remotos (por ejemplo, cámaras de seguridad, fuentes de noticias, etcétera).

La siguiente exposición describe la materia objeto de la invención con respecto al dispositivo electrónico 110, por ejemplo un teléfono celular, que captura datos de imágenes en forma de una representación digital 141 de uno o

más objetos físicos 120A a 120B en un entorno físico. Debe apreciarse que las técnicas que se dan a conocer posteriormente se pueden adaptar de manera sencilla a otras modalidades de datos, incluyendo sonido, vídeo en movimiento, datos biométricos, datos de posición, u otros datos que se pueden capturar a través de sensores, o se pueden obtener de otra manera a partir de fuentes de datos. Adicionalmente, el ejemplo presentado se centra en objetos físicos 120A y 120B del mundo real. No obstante, los objetos de autenticación también pueden comprender objetos virtuales reproducidos en un sistema de ordenador, un objeto virtual en un mundo de un juego en línea, por ejemplo, un objeto de realidad aumentada, u otros tipos de objetos virtuales.

En el ejemplo mostrado, el dispositivo electrónico 110 captura una representación digital 141 en forma de una imagen que refleja una interacción 105 con una escena 100 que comprende una planta (es decir, objeto 120A) y un documento representado como un permiso de conducir (es decir, el objeto 120B). La planta y el permiso de conducir representan objetos del mundo real ilustrativo que se pueden usar como clave para desbloquear el contenido 193 u obtener acceso al control sobre el contenido 193. La interacción 105 puede incluir meramente la captura de una imagen así como interacciones más complejas. Las interacciones ejemplificativas 105 podrían incluir jardinería, atender a una visita en el dentista, compras en una tienda de bricolaje, u otro tipo de interacciones multi-modales. Cada interacción 105 puede quedar determinada por una firma de datos de sensor, por comparación con interacciones conocidas en una base de datos de interacciones (no mostrada) o a través de un tipo de interacción seleccionado por el usuario.

El dispositivo electrónico 110 obtiene la imagen, u otra representación digital 141, y puede procesar los datos según sea necesario. Debe apreciarse que la representación digital 141 puede incluir datos de sensores sin procesar, datos de sensores procesados (por ejemplo, un archivo de imagen), datos de sensores analizados (por ejemplo, conjunto de datos reducido), u otra información obtenida a partir de la representación digital 141. A continuación, la representación digital 141 se puede presentar a la plataforma 140 de reconocimiento configurada para recibir, u obtener de otro modo, la representación digital 141. La representación digital se puede transmitir a través de una red (por ejemplo, WAN, LAN, Internet, Red Celular, etcétera) a la plataforma 141 de reconocimiento usando protocolos conocidos (por ejemplo, HTTP, FTP, SSL, SSH, etcétera), u otros protocolos privativos. En algunas realizaciones, el dispositivo electrónico 110 comprende la plataforma 141 de reconocimiento. Además, debe apreciarse que cada uno de los elementos del sistema dado a conocer, tiene funciones o responsabilidades que pueden estar distribuidas por el ecosistema. Por ejemplo, el agente 180 de autenticación puede estar dispuesto dentro del dispositivo electrónico 110, o puede estar funcionando como un servidor remoto que proporciona servicios de autenticación por una tarifa. Todavía adicionalmente, las funciones y responsabilidades de un elemento individual pueden estar distribuidas por múltiples dispositivos dentro del ecosistema. Por ejemplo, la base 195 de datos de contenido podría tener secciones dispuestas dentro del dispositivo electrónico 110, en la plataforma 140 de reconocimiento, o incluso en servicios de terceros remotos (por ejemplo, un motor de búsqueda, un sitio de compras, etcétera).

La plataforma 140 de reconocimiento recibe la representación digital 141, e intenta identificar los objetos 120A ó 120B en la escena o entorno 100, según se representan en la representación digital 141. Por ejemplo, la planta y el permiso de conducir. La plataforma 140 de reconocimiento puede analizar la representación digital 141 para extraer una o más características 160 relacionadas con objetos 120A ó 120B. En algunas realizaciones, las características 160 pueden incluir atributos de objeto asociados a los objetos 120A ó 120B. Se contempla también que las características 160 puedan incluir atributos obtenidos a partir de los datos de la representación digital 141. Con respecto a las imágenes, las características 160 podrían incluir Transformada de Características Invariantes a la Escala (SIFT), Puntos Clave Escalables Invariantes, Robustos y Binarios (BRISK), Características Robustas Aceleradas (SURF), u otros tipos de características obtenidas a partir de los datos de imágenes. En algunas realizaciones, las características 160 podrían incluir un valor *hash* calculado a partir de por lo menos una parte de la imagen, o una parte de la representación digital 141, incluso a partir de otras modalidades. Un valor *hash* aceptable puede incluir un valor *hash* perceptual donde el valor *hash* perceptual es similar para contenido similar (véase el URL www.phash.org). Los valores *hash* perceptuales de ejemplo incluyen un valor *hash* de imagen MH de longitud fija, un valor *hash* de vídeo de longitud variable con Transformada Discreta de Coseno (DCT), un valor *hash* de imagen con DCT, un valor *hash* de imagen radial, un valor *hash* de imagen basado en histogramas, o un valor *hash* de audio de bark. Las características 160 también podrían incluir palabras o términos generados a través de Reconocimiento Automático del Habla (ASR), valores biométricos (por ejemplo, respiración, ritmo cardiaco, presión sanguínea, características faciales, etcétera), información de posición (por ejemplo, GPS, triangulación, movimiento inercial, datos de Iridium no GPS, etcétera), u otros atributos obtenidos a partir de muchas modalidades.

Las características 160 también pueden depender de la modalidad de los datos de interacción según se representa en la representación digital. Las características 160 de objetos, ilustrativas, adicionales, pueden incluir información relacionada con el tiempo, la posición, acontecimientos informativos, condiciones meteorológicas, temperatura, presión, firmas biométricas, señales de voz o audio, u otros tipos de modalidad. Con independencia del tipo de características 160 de objetos, o de cómo se generan las características 160 de objetos, la plataforma 140 de reconocimiento puede usar las características 160 de objetos para determinar la naturaleza de los objetos 120A ó 120B del mundo real. En algunas realizaciones, la plataforma de reconocimiento reconoce objetos 120A y 120B buscando en una base de datos de objetos sobre la base de las características de los objetos. En las patentes de Estados Unidos, de propiedad conjunta, 7.016.532; 7.477.780; 7.680.324; 7.403.652; 7.565.008; 7.899.243; 7.881.529; 7.899.252; y otras de la misma familia, se describen técnicas adecuadas para reconocer objetos.

La plataforma 140 de reconocimiento puede proporcionar las características 160 de objetos al agente 180 de autenticación. El agente 180 de autenticación puede usar características 160 de objetos, u otra información de objetos, para determinar si realmente el objeto 120A ó 120B del mundo real es un objeto de autenticación válido discriminando el objeto con respecto a otros de la escena según se representa con la representación digital 141. Características 160 de objetos o información adicional se pueden usar para construir una consulta con el fin de buscar, en la base 150 de datos de objetos de autenticación, objetos que se consideren como objetos de autenticación válidos. El agente 180 de autenticación puede usar la consulta para obtener un conjunto de resultado de objetos de autenticación conocidos que presentan características de objeto que satisfacen la consulta. Así, la búsqueda en la base de datos se puede utilizar para discriminar entre objetos representados en la representación digital 141, con el fin de determinar si los mismos son objetos de autenticación válidos. En el ejemplo mostrado, la planta o el permiso de conducir (o ambos) se podría validar por medio del agente 180 de autenticación, como objetos de autenticación válidos reales con respecto a una o más propiedades de la interacción 105. Por ejemplo, la planta y el permiso de conducir podrían solamente ser válidos para el usuario específico según se determine a partir de información de la cuenta de usuario, objetos de autenticación registrados, el dispositivo electrónico específico del usuario según se determine a partir de un identificador de dispositivo, en las coordenadas GPS o datos de posición actuales, o durante un periodo de tiempo especificados. Todos estos factores, y más, se pueden poner en uso para determinar si los objetos 120A ó 120B del mundo real son de hecho objetos de autenticación válidos para activar contenido. Tal como se ha mencionado previamente, los objetos virtuales también pueden representar objetos de autenticación válidos a través de técnicas similares.

Los objetos de autenticación válidos pueden incluir una amplia variedad de objetos. Los objetos 2D de ejemplo pueden incluir soportes impresos (por ejemplo, un permiso de conducir, un pasaporte, una firma, un cheque, un documento, un cartel, una valla publicitaria, una fotografía, una imagen representada, un libro, un periódico, una revista, etcétera, una sombra, una imagen representada en una pantalla de visualización (por ejemplo, pantalla de ordenador, televisión, sistema de juego, valla publicitaria electrónica, pantalla de cine, quiosco interactivo, máquina expendedora, pantalla de visualización médica, etcétera), un objeto virtual representado, una tarjeta de crédito, u otros objetos aproximadamente planos. Los objetos 3D de ejemplo que se podrían usar como objeto de autenticación válido pueden incluir una persona, una cara, un animal, una prenda de vestir, un vehículo, un edificio, un juguete, una planta, un dispositivo informático, una construcción, un alimento, una figurita, un modelo impreso, un robot, una herramienta, u otros objetos físicos que tengan una anchura, profundidad o longitud sustanciales. Todavía adicionalmente, los objetos de autenticación válidos también pueden incluir aspectos temporales. Los objetos de ejemplo que cambien con el tiempo incluyen palabras pronunciadas, vídeos, música, gestos, movimiento articulado de dispositivos (por ejemplo, juguetes, robots, etcétera), u otros objetos que cambien con el tiempo.

Una vez que el agente 180 de autenticación determina que dos o más del objeto físico 120A ó 120B se corresponden con objetos de autenticación válidos, el agente 180 de autenticación puede determinar uno o más niveles 183 de acceso a contenido, basándose en una yuxtaposición de características 160, características de autenticación, u otra información disponible. Los niveles 183 de acceso determinan un alcance de contenido 193 a activar para la interacción actual 105, un alcance de control sobre el contenido, un alcance de posibles interacciones futuras con el contenido 193 en el entorno 100. Los niveles 183 de acceso se pueden obtener basándose en una tabla de búsqueda o se pueden calcular sobre la base de lo bien que coinciden las características 160 con características de autenticación relevantes mapeadas con niveles 183 de acceso a contenido. Por ejemplo, si el permiso de conducir está delante de la planta, entonces podría activarse una gama completa de contenido 193. Si el permiso de conducir está detrás de la planta, entonces podría activarse un contenido mínimo 193. Un planteamiento de este tipo permite que los publicadores de contenido determinen cómo o con qué alcance puede distribuirse su contenido 193. Además, la colocación del objeto 120A con respecto al objeto 120B puede controlar cómo se accede al contenido 193. Para continuar con el ejemplo previo, cuando el permiso de conducir se mueve más hacia adelante de la planta, de manera que el permiso de conducir abarca una mayor parte de la imagen, podría ordenarse el contenido 193 que avanzase rápidamente. Si el permite de conducir se mueve detrás de la planta, podría ordenarse al contenido 193 que rebobinase. En tales casos, la distancia obtenida en el espacio de interacción entre el objeto 120A y 120B puede usarse para controlar una velocidad de reproducción.

Se pueden proporcionar niveles 183 de acceso a contenido, o información relacionada con niveles 183 de acceso, al servidor 190 de contenido que almacena una o más partes del contenido 193 en la base 195 de datos de contenido. La información de niveles de acceso informa al servidor 190 de contenido sobre qué contenido 193 ó el alcance del contenido 193 a presentar al usuario de dispositivos electrónicos 110 u otros dispositivos de salida. Así, el contenido identificado 193 se activa para que sea consumido por el usuario. El dispositivo de salida podría incluir el dispositivo electrónico 110, un electrodoméstico, una impresora, un robot, una máquina, un vehículo, o un tipo de dispositivo capaz de presentar el contenido.

En algunas realizaciones, el servidor 190 de contenido puede enviar una señal o instrucción al dispositivo electrónico 110, u otro dispositivo de salida, para instanciar la máquina virtual 112. En el ejemplo mostrado, la máquina virtual 112 se representa ampulosamente como una caja externa al dispositivo de salida (es decir, el dispositivo electrónico 110). No obstante, alguien versado en la materia apreciará que la máquina virtual 112 se instancia dentro de la memoria o procesador del dispositivo electrónico 110. La máquina virtual 112 puede permanecer bajo el control del servidor 190 de contenido, el agente 180 de autenticación, o el proveedor de contenido, de acuerdo con una o más

reglas determinadas por niveles 183 de acceso. A continuación, el servidor 190 de contenido puede ordenar a la máquina virtual 112 que presente contenido 193 en el dispositivo electrónico 110 de salida. A garantizar que el servidor 190 de contenido, u otros elementos de la infraestructura, controla la máquina virtual 112 ó sus funciones, los derechos del proveedor de contenido permanecen protegidos al mismo tiempo que se permite también que un consumidor de contenido adquiera contenido 193 bajo demanda, mediante el reconocimiento de objetos de autenticación válidos. En la patente de Estados Unidos 7.181.617, de Wise, titulada “Remote Virtual Medical Diagnostic Imaging Viewer”, presentada el 10 de junio de 2002; la patente de Estados Unidos 7.685.417, de Wise, titulada “Remote Data Viewer”, presentada el 19 de enero de 2007; la publicación de solicitud de patente de Estados Unidos 2008/0263048, de Wise, titulada “File Access Management System”, presentada el 16 de abril de 2008; y la publicación de solicitud de patente de Estados Unidos 2010/0169642, de Wise, titulada “Remote Data Viewer”, presentada el 12 de marzo de 2010, se describen técnicas adecuadas para instanciar la máquina virtual 112 y controlar la presentación de contenido.

Se considera que la materia objeto de la invención incluye la instanciación o lanzamiento de la máquina virtual 112 con propiedades determinadas a partir de características 160 de objetos de autenticación. Dichas características pueden dictaminar el acceso de un consumidor al contenido presentado o reproducido 193. Por ejemplo, la yuxtaposición de los objetos del mundo real uno con respecto a otro, podría provocar que la máquina virtual 112 se instanciase de una manera que permitiese que el consumidor de contenido desplazase en el tiempo del contenido (por ejemplo, avance rápido, rebobinado, pausa, etcétera).

La Figura 2 proporciona una visión general más detallada de la discriminación entre objetos 220 de autenticación y objetos 230 que no son de autenticación, dentro del entorno 200. Un individuo hace uso del dispositivo 210 para interaccionar con el entorno 200, que puede incluir múltiples objetos. Los objetos en el entorno podrían incluir uno o más objetos 220 de autenticación u objetos 230 que no son de autenticación. El dispositivo 210 obtiene una representación digital 241 que comprende datos, posiblemente datos multi-modales, que representan aspectos del entorno 200. El dispositivo 210 transmite la representación digital 241 a través del enlace 215 de comunicaciones a la plataforma 240 de reconocimiento. El enlace 215 de comunicaciones podría incluir una red (por ejemplo, inalámbrica, por cable, Internet, PAN, VPN, WAN, etcétera) cuando la plataforma 240 de reconocimiento está distante del dispositivo 210, o podría incluir una conexión interna (por ejemplo, un bus, una memoria compartida, un registro, una API, etcétera), si la plataforma 240 de reconocimiento está dispuesta dentro del dispositivo 210. Debe indicarse que la plataforma 240 de reconocimiento se puede acoplar con un agente de autenticación, un servidor de contenido, el dispositivo 210, servicios remotos, u otras plataformas informáticas. En aras de la presente descripción, la plataforma 240 de reconocimiento debería considerarse de manera que incluye un agente de autenticación.

La plataforma 240 de reconocimiento aplica una o más técnicas de análisis sobre la representación digital 241 para generar características 243 a partir de la representación digital 241. En algunas realizaciones, las características 243 se pueden considerar propiedades de la propia representación digital 241, más que características del entorno 200. Por ejemplo, pueden analizarse datos de imágenes para generar características de imágenes que incluyen posiblemente descriptores (por ejemplo, balance de color, histogramas, ondículas, características SIFT, puntos clave de BRISK, descriptores de SURF, descriptores de ORB, etcétera), descriptores de movimiento obtenidos a partir de datos de movimiento (por ejemplo, vSLAM, GPS, etcétera), parámetros de audio (por ejemplo, amplitud, fase, frecuencia, etcétera), u otros tipos de características 243. A continuación, dichas características pueden ser usadas por el discriminador 247 para discriminar objetos 220 de autenticación con respecto a objetos 230 que no son de autenticación.

En algunas realizaciones, el discriminador 247 puede funcionar como un motor de búsqueda que recibe la consulta, y presenta la consulta a la base 250 de datos de objetos conocidos. Como respuesta a la consulta, la base 250 de datos de objetos conocidos devuelve un conjunto de resultado de información de autenticación relacionada con objetos de autenticación que presentan atributos que satisfacen la consulta. La base 250 de datos de objetos conocidos se puede configurar para almacenar información de objetos de autenticación, posiblemente indexada de acuerdo con un espacio de nombres común al cual se adhieren las características 243. El espacio de nombres común puede considerarse un esquema definido de tal manera que describe un espacio de interacción posible. El espacio de interacción puede considerarse como un espacio multi-dimensional, en el que cada dimensión representa una posible forma o modalidad de datos de sensores. El espacio de interacción se puede definir en términos de información de posición (por ejemplo, coordenadas; X, Y o Z; longitud, latitud; etcétera), información de tiempo, información de orientación, información biométrica, u otra información del espacio de interacción. Así, la información de objetos de autenticación se puede almacenar o recuperar basándose en características SIFT o conglomerados de características, firmas de audio, firmas de sensores, coordenadas de localización o posición, firmas de orientación, firmas biométricas, información de perfiles de usuario, u otros aspectos dentro del espacio de interacción.

El discriminador 247 recibe el conjunto de resultados de la base 250 de datos de objetos conocidos, y realiza una discriminación entre objetos dentro del entorno 200 consultando la información devuelta de objetos de autenticación. El discriminador 247 compara características 243, u otra información disponible para el sistema o a través de la representación digital 241, con información de objetos de autenticación del conjunto de resultado para identificar todos los objetos conocidos. Si se hallan objetos conocidos, y se considera que los mismos son objetos 249 de

autenticación válidos con respecto a la interacción, entonces la plataforma 240 de reconocimiento obtiene uno o más conjuntos de características 260 de autenticación con respecto a cada objeto 249 de autenticación válido.

Como ejemplo más concreto, considérese un escenario en el que el dispositivo 210 captura una imagen del entorno 200, la cual presenta múltiples objetos tal como se representa en la Figura 2. Probablemente, la representación digital 241 comprendería datos de imagen, entre otras modalidades. No obstante, en aras de la descripción, este ejemplo se centrará en los datos de imagen. La plataforma 240 de reconocimiento podría analizar los datos de imagen, y generar una serie de descriptores de imagen SIFT o BRISK relacionados con los datos de imagen. A continuación, los descriptores se pueden trasladar al discriminador 247, el cual, a su vez, genera una consulta en función de los descriptores de imagen, y presenta la consulta a la base 250 de datos de objetos conocidos. La consulta puede incluir descriptores de imagen reales junto con otra información. La base 250 de datos de objetos conocidos puede devolver un conjunto de información de objetos conocidos relacionados con objetos representados visualmente conocidos *a priori* de los cuales se considera que presentan descriptores de imagen similares, por lo menos dentro de un nivel de confianza, según requiera la consulta. Por ejemplo, la base 250 de datos de objetos conocidos podría devolver información relacionada solamente con objetos 220 de autenticación, o podría devolver información relacionada con objetos adicionales además de los objetos 220 de autenticación; por ejemplo, objetos 230 que no sean de autenticación. Debe apreciarse que este planteamiento se puede usar para reconocer esencialmente cualquier objeto en el entorno 200, si los objetos son ya conocidos o están registrados en la base 250 de datos de objetos conocidos. El planteamiento resulta ventajoso puesto que permite la utilización de bases de datos de objetos existentes o de terceros, en lugar de disponer de una base de datos privativa. Las bases de datos de objetos de terceros ilustrativas incluyen Google® Goggles™, in8™ Mobile's iD (véase el URL www.in8.com/#big-id) Amazon, u otras bases de datos de objetos de terceros.

Para continuar con el ejemplo, el discriminador 247 consulta la información de objetos devuelta, y, basándose en los datos de imagen, discrimina cuáles de los objetos son realmente objetos 290 de autenticación válidos. Por ejemplo, si todos los objetos del entorno 200 se representan en el conjunto de resultados, la información relacionada con los objetos 220 de autenticación se puede etiquetar con metadatos u otro tipo de datos que indiquen que son de hecho objetos 249 de autenticación válidos. Debe apreciarse que los objetos 249 de autenticación válidos incluyen objetos 220 de autenticación, una parte de los objetos 220 de autenticación, u otros objetos además de aquellos que estén en los datos de imagen; por ejemplo, una persona identificada a partir de una huella vocal.

Continuando con el ejemplo, con independencia de cómo se discriminan los objetos, la plataforma 240 de reconocimiento obtiene uno o más de los conjuntos 260 de características de autenticación a partir de las características 243 y los objetos 240 de autenticación válidos. Con respecto a los datos de imagen y al ejemplo presentado, los conjuntos 260 de características de autenticación podrían incluir un primer conjunto de características de autenticación que se corresponda con la planta, y un segundo conjunto de características de autenticación que se corresponda con el permiso de conducir (por ejemplo, un documento).

La Figura 3 ilustra un subconjunto de posibles análisis que podrían generar conjuntos de características 360 de autenticación. En el ejemplo, los conjuntos de características 360 de autenticación incluyen el conjunto 360A que se corresponde con el objeto planta 349A, el conjunto 360B que se corresponde con los objetos 349B de documento, y el conjunto 360C que se corresponde con el objeto 349C de audio. Cada uno de los objetos 349A a 349C se puede representar por medio de una o más modalidades de datos dentro de la representación digital 341. Por ejemplo, la representación digital 341 podría incluir datos de imagen (por ejemplo, JPG, PNG, BPM, imagen fija, vídeo, etcétera) que representan el objeto 349A y 349B. Además, la representación digital 341 podría incluir datos de audio (por ejemplo, WAV, MP3, una grabación, etcétera) que representen sonidos asociados al entorno.

Cada modalidad de datos dentro de la representación digital 341 se puede analizar de acuerdo con una o más técnicas 343 de análisis asociadas a la modalidad. Pueden analizarse datos de imagen usando técnicas que incluyen posiblemente una o más de las siguientes: SIFT, BRISK, SURF, SLAM, vSLAM, ondículas, reconocimiento óptico de caracteres (OCR), u otras técnicas para generar conjuntos 360A ó 360A de características. Debe apreciarse que los conjuntos 360A ó 360B de características podrían incluir características obtenidas sin procesar (por ejemplo, descriptores en una posición específica en los datos de imagen o en el espacio de interacción) o características indirectas o deducidas. Las características indirectas o deducidas podrían incluir texto obtenido a partir de la aplicación del OCR a los datos de imagen, o metadatos o etiquetas basados en una búsqueda de objetos. Por ejemplo, el conjunto 360A de características podría incluir una etiqueta que denominase el tipo, el género o la especie del objeto planta 349A, aún cuando dicha información no esté presente en forma textural en los datos de imagen. Además, el conjunto 360C de características podría incluir solamente palabras que hayan sido reconstruidas mediante técnicas de reconocimiento automático del habla (ASR) y grabadas con respecto al tiempo. Cada uno de los conjuntos de características 360 de autenticación se ilustra de manera que presenta numerosas características. Debe apreciarse que un conjunto de características 360 de autenticación puede incluir una, tres, siete, diez o más características en función de las técnicas usadas para generar las mismas. Por ejemplo, un conjunto de características basado en imágenes podría incluir más de cien, o incluso más de mil, características. Aunque los conjuntos de características de autenticación pueden incluir datos de símbolos (por ejemplo, texto, alfanuméricos, códigos de barras, códigos QR, códigos matriciales, códigos de colores, etcétera), se contempla que el conjunto de características pueda carecer de información obtenida a partir de una etiqueta simbólica asociada a

los objetos de autenticación válidos. Por ejemplo, el conjunto de características puede carecer de cualquier dato de código de barras asociado al objeto de autenticación válido y seguir siendo útil para activar el contenido.

Los conjuntos de características 360 de autenticación se presentan como objetos diferenciados y gestionados de manera independiente, dentro de la Figura 3. Cada uno de los conjuntos 360 se podría usar individualmente para identificar o autenticar objetos respectivos 349A a 349C. Otros conjuntos 360 podrían combinarse para crear un token o clave colectivo con el fin de identificar o autenticar un usuario o una interacción solicitada. Todavía adicionalmente según se da a conocer en la presente, la yuxtaposición de los conjuntos 360 unos con respecto a otros, en el espacio de interacción, da origen a un sistema rico de autenticación, autorización, mando, control o gestión, capaz de activar contenido.

La Figura 4 ilustra la obtención de un objeto 470 de yuxtaposición a partir de múltiples conjuntos 460A, 460B y 460C de características de autenticación, a los que se hace referencia colectivamente como conjuntos 460 de características de autenticación. Tal como se ha mencionado previamente, los conjuntos 460 de características de autenticación existen en el espacio 400 de interacción. El espacio 400 de interacción se ilustra como un espacio físico (es decir, ejes X, Y) y que tiene un componente de tiempo (es decir, eje t) para facilitar la descripción. Debe apreciarse que el espacio 460 de interacción podría tener otras dimensiones, que incluyen posiblemente intención derivada, contexto, demografía, u otros aspectos relacionados con la interacción. Cada punto en el espacio 400 de interacción se podría representar con un vector o una N-Tupla.

Puede considerarse que cada uno de los conjuntos 460 de características de autenticación existe dentro de los espacios de interacción. Por ejemplo, el conjunto 460A podría representar una o más características SIFT obtenidas a partir de un objeto de planta representado visualmente (véase la Figura 3, conjunto 360A), donde cada característica se corresponde con una posición relativa en un espacio físico-tiempo según se muestra. La posición de las características SIFT se podría determinar a través de cálculos de profundidad de campo, basados posiblemente en las técnicas dadas a conocer en la publicación de solicitud de patente de Estados Unidos 2012/0163672, de McKinnon, titulada “Depth Estimate Determination, Systems and Methods”, presentada el 7 de junio de 2012. La posición de las características podría obtenerse también a partir del uso del vSLAM cuando haya disponibles datos de movimiento. Todavía adicionalmente, la posición con respecto al tiempo se puede determinar basándose en sellos de tiempo dentro de la representación digital, sellos de tiempo basados en observaciones, o incluso cuando llegan los datos. El origen del espacio de acciones de interacción se puede determinar a partir de datos de posición del dispositivo de captura (por ejemplo, GPS, movimiento inercial, etcétera), a partir de la posición u orientación del dispositivo de captura con respecto al fondo, u otra información basada en la posición. Así, cada conjunto 460A, 460B ó 460C de características existe en forma de puntos o posiciones dentro del espacio 400 de interacción.

Los conglomerados de características en los conjuntos 460 de características se pueden tratar como un grupo identificando los conglomerados con respecto a un objeto de autenticación. Los conglomerados se pueden descubrir u obtener dentro del espacio de interacción, por medio de una o más técnicas de conglomerados (*cluster*). Por ejemplo, podrían hallarse conjuntos 460A de características mediante el uso de K medias (es decir, conglomeración basada en centroides), conglomeración de EM (es decir, conglomeración basada en distribuciones), DBSCAN (es decir, conglomeración en densidad), CLIQUE o SUBCLU (es decir, conglomeración de subespacios en datos de más dimensiones), u otros tipos de técnicas de conglomeración. Así, cada conglomerado se puede identificar como asociado a un objeto de autenticación válido. Además, los conglomerados pueden tener una extensión sobre el espacio; centro de “masas”, centroide, centro, número, anchuras, distancia, densidad, longitud, amplitud, duración, u otra propiedad. A continuación, dichas propiedades se pueden usar para determinar atributos de yuxtaposición, y se consideran ventajosas cuando se determina el nivel de acceso al contenido.

La yuxtaposición entre conjuntos 460 de características se puede determinar basándose en varios aspectos o propiedades del espacio 400 de interacción. En el ejemplo mostrado, la yuxtaposición se puede determinar sobre la base de la orientación relativa 461 de uno de los conjuntos 460 de características con respecto a otro. Una vez que se ha seleccionado una dirección preferida de un conjunto de características (es decir, determinar qué elementos de un conjunto se consideran una “cima” o “parte superior” preferida del conjunto), la orientación se podría representar basándose en ángulos absolutos con respecto al origen del espacio de interacción, o se podría representar basándose en ángulos relativos de un conjunto a otro. La orientación 461 se podría representar mediante un conjunto de Ángulos de Euler con respecto al espacio 400 de interacción. Además, la yuxtaposición de puede determinar basándose en la posición relativa 463 entre conjuntos 460 de características. La posición relativa 463 se podría representar como un vector que tiene elementos correspondientes a cada dimensión del espacio de interacción, donde el valor de cada elemento representa una distancia o una diferencia en la distancia. En un espacio tridimensional, la posición relativa 463 entre el conjunto 460A y 460C de características se podría representar como $V = \{X_C – X_A, Y_C – Y_A, Z_C – Z_A\}$. La posición relativa también se podría representar basándose en coordenadas absolutas con respecto al origen del espacio de interacción. Todavía adicionalmente, la yuxtaposición entre conjuntos 460 de características se podría basar en el tiempo relativo 465. El tiempo relativo 465 se puede expresar basándose en el momento en el que se produjo cada uno de los conjuntos 460 de características o en el momento en el que se detectaron con respecto a la interacción. Debe apreciarse que también se pueden usar otras dimensiones del espacio 400 de interacción para calcular u obtener una yuxtaposición entre conjuntos 460 de

características.

La yuxtaposición 470 representa una agregación de información 470A, 470B y 470C de yuxtaposición, obtenida a partir de conjuntos 460A, 460B, y 460C de características, respectivamente. La información de yuxtaposición se puede considerar un conjunto de atributos de yuxtaposición que se refieren a la interacción actual de interés. Los atributos pueden incluir nombres de objetos identificados, número de características relevantes en un conjunto de características, tipos de objetos o características, un centroide del conjunto de características, valores o posiciones relativos, u otros atributos de yuxtaposición.

La Figura 5 ilustra un posible método de establecimiento, por parte del agente 580 de autenticación, de uno o más niveles 583 de acceso para contenido 593. En el ejemplo mostrado, el agente 580 de autenticación utiliza una o más yuxtaposiciones 570 como base para generar una consulta u otros criterios usados para seleccionar un nivel de acceso. Por ejemplo, la consulta podría comprender identificadores de objetos (por ejemplo, nombre, marca, tipo, GUIDs, UUIDs, números de serie, etcétera) u otros atributos de objetos junto con atributos de yuxtaposición referentes a conjuntos de características de autenticación correspondientes (por ejemplo, posición, conglomerados, grupos, orientaciones, tiempo, etcétera). El agente 580 de autenticación puede presentar la consulta a la base 550 de datos de autenticación, la cual, a su vez, devuelve información de contenido que es desbloqueada por la yuxtaposición 570. La información de contenido puede incluir niveles 583 de acceso, los cuales se pueden usar para acceder a uno o más del contenido 593.

Los niveles 583 de acceso representan un grado o alcance según el cual un usuario puede interaccionar con el contenido 593. Tal como se ilustra, el contenido 593 podría comprender múltiples niveles de acceso, en función de la naturaleza del contenido, donde cada nivel se puede activar basándose en la yuxtaposición 570. Por ejemplo, si el contenido 593 comprende un juego promocional de realidad aumentada, accesible por medio de un teléfono celular, el nivel de acceso al juego se puede determinar mediante diferentes yuxtaposiciones de objetos de autenticación válidos, por ejemplo una lata de bebida y un cartel NBA de los Lakers®. A medida que el usuario se posiciona con la lata de bebidas en torno al cartel o con respecto a características del cartel (por ejemplo, imágenes de jugadores, logotipos, etcétera), el usuario puede obtener un mayor acceso. Quizás la colocación de una lata de Pepsi® a la derecha de Kobe Bryant se correspondía con el nivel de acceso 1, el cual simplemente al usuario observar o reproducir contenido del juego. Si el usuario coloca una lata de Coke® a la derecha de Kobe Bryant, tal vez el usuario lograría el nivel de acceso 2, y recibiría un cupón gratuito o una promoción. Sin embargo, el movimiento adicional de la lata a posiciones relativas podría ofrecer un mayor control autorizando al usuario que desplazase el contenido en el tiempo, que iniciase o participase en una transacción, que copiase o grabase contenido, que editase contenido, que compartiese el contenido, que interaccionase de manera directa o indirecta con el contenido, o que accediese de otra manera al contenido. De este modo, el dispositivo de salida puede presentar una promoción asociada a un producto como contenido 593, especialmente cuando la promoción está asociada al objeto de autenticación válido. Aunque el ejemplo usa una lata de bebida de manera ilustrativa, la promoción podría incluir un cupón, un mensaje publicitario, una oferta, una rebaja, un número de lotería, un anuncio, u otro tipo de promoción.

Debe apreciarse que los niveles 583 de acceso podrían representar medidas de seguridad además de medidas de control. Un usuario puede posicionar dos objetos uno con respecto a otro, y registrar la configuración en el sistema como token para desbloquear una cuenta bancaria o autorizar una transacción. El usuario también podría registrar una segunda disposición que podría ser similar a la primera disposición, aunque activaría el contenido de acuerdo con un nivel 583 de acceso diferente. Por ejemplo, la colocación de un permiso de conducir a la derecha de una planta podría activar una transacción con la cuenta bancaria de una persona. No obstante, en caso de que un individuo se encontrase bajo coacción, resultaría beneficioso simular la activación de la transacción. Quizás la colocación del permiso de conducir a la izquierda de la planta podría activar una transacción falsa mientras que se notifica también a las autoridades la aparición de actividades maliciosas.

El contenido 593 puede incluir un amplio espectro para modalidades o tipos de contenido. Los ejemplos de tipos de contenido pueden incluir software o módulos de aplicaciones, datos de imagen, datos de vídeo, datos de audio, historiales médicos, datos de juegos, datos promocionales, información de bienes y servicios, datos de realidad virtual o aumentada, órdenes, instrucciones, instrucciones u órdenes robóticas, u otros tipos de datos. Otros ejemplos de contenido incluyen información de transacciones, información de entretenimiento, información de noticias, información deportiva, información promocional, información médica, información de seguridad, información de juegos, información de aplicaciones, información sanitaria, información de la oficina o del trabajo, u otros tipos de información. Las modalidades de ejemplo pueden incluir auditiva, visual, cinestésica, gestos, olfativa, táctil, gustativa, información de sensores, u otros tipos de modalidades. Adicionalmente, el contenido puede incluir múltiples tipos de medios y se puede considerar como contenido trans-media.

La Figura 6 presenta un método 600 para activar contenido basándose en las técnicas dadas a conocer. La etapa 610 incluye la habilitación de un dispositivo electrónico para acceder a un agente de autenticación. En algunas realizaciones, un usuario puede instalar instrucciones de software en una memoria legible por ordenador, no transitoria, del dispositivo electrónico, donde las instrucciones se ejecutan en un procesador para proporcionar los servicios del agente de autenticación. El agente de autenticación puede funcionar como aplicación autónoma, como módulos dentro de una biblioteca, o incluso como una parte integral de un sistema operativo. En otras realizaciones, se puede acceder al agente de autenticación a través de una red donde uno o más dispositivos informáticos remotos

proporcionan acceso a los servicios del agente de autenticación. Por ejemplo, un agente de autenticación puede funcionar como servicio de tarificación independiente que actúa como sistema virtualizado basado en la nube (por ejemplo, PaaS, IaaS, SaaS, etcétera). Los dispositivos electrónicos del ejemplo pueden incluir teléfonos inteligentes, vehículos, electrodomésticos, quioscos interactivos, sistemas de juego, máquinas expendedoras, dispositivos médicos, ATMs, u otros tipos de dispositivos electrónicos.

La etapa 620 incluye el dispositivo electrónico obteniendo una representación digital de una interacción con un entorno, físico o virtual, que incluye una pluralidad de objetos. El dispositivo electrónico puede obtener la representación digital a partir de uno o más sensores. Los sensores pueden ser internos o estar integrados con el dispositivo electrónico, o podrían ser remotos con respecto al dispositivo. Por ejemplo, en una realización en la que el dispositivo electrónico comprende un teléfono inteligente, los sensores pueden incluir una cámara integrada, un acelerómetro, una pantalla táctil, un micrófono, un sensor GPS, un transceptor inalámbrico, u otros sensores. Los sensores remotos pueden incluir cámaras de seguridad, sensores meteorológicos, sensores médicos, sondas de Efecto Hall, u otros dispositivos de captación a los que se pueda acceder por medio de un enlace de comunicaciones externo al dispositivo electrónico. La interacción puede incluir grabar audio, comprar un producto, capturar una imagen, compartir contenido en una red social, hacer funcionar el dispositivo electrónico, jugar a un juego, jardinería, u otro tipo de interacción que pueda ser captada.

Se considera que la representación digital comprende datos representativos del entorno según se obtienen a partir de los diversos sensores. Teniendo en cuenta que los sensores pueden capturar una amplia variedad de modalidades de datos, el método puede incluir además obtener unos datos multi-modales como parte de la representación digital. Por ejemplo, los datos multi-modales pueden incluir dos o más de datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos químicos, datos médicos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración, datos de rumbo, u otros tipos de datos según sugiera la etapa 625.

La etapa 630 puede incluir discriminar por lo menos dos objetos diferentes de entre la pluralidad de objetos en el entorno, como objetos de autenticación válidos basándose en la representación digital. En algunas realizaciones, una plataforma de reconocimiento analiza la representación digital para convertir las señales digitales en uno o más atributos o propiedades, que, a continuación, se pueden usar para identificar o reconocer objetos dispares posiblemente mediante una búsqueda en base de datos. La plataforma de reconocimiento puede reconocer múltiples objetos dentro del entorno comparando objetos conocidos con los atributos obtenidos. A continuación, los objetos reconocidos se pueden discriminar como objetos de autenticación válidos con respecto a objetos que no son de autenticación, mediante la consulta de información de objetos almacenada en la base de datos de objetos conocidos o en un registro de objetos de autenticación. Cuando se encuentra una coincidencia, y la coincidencia está registrada como objeto de autenticación válido, la plataforma de reconocimiento puede notificar al agente de autenticación, de que al menos algunos de los objetos del entorno que presentan coincidencias son de hecho objetos de autenticación válidos. Debe apreciarse que la plataforma de reconocimiento podría estar dispuesta dentro del dispositivo electrónico o también podría estar dispuesta en servidores remotos, posiblemente acoplada con el agente de autenticación a través de una red.

La etapa 640 incluye obtener por lo menos un primer conjunto de características de autenticación a partir de la representación digital y asociadas al primer objeto de autenticación válido, y obtener un segundo conjunto, diferente, de características de autenticación a partir de la presentación digital y asociadas al segundo objeto de autenticación válido. Los conjuntos de características de autenticación pueden incluir los atributos o propiedades obtenidos de la representación digital, o pueden incluir características indirectas o deducidas. Los atributos obtenidos pueden incluir características, tales como descriptores de imagen o puntos clave, propiedades de señales de audio, intensidades de señales biométricas, u otras características del estilo. Las características indirectas o deducidas se pueden obtener mediante la obtención de información de objetos relacionada con los objetos reconocidos; un nombre, una clase, una marca, una identidad, metadatos, u otra propiedad. Además, tal como sugiere la etapa 641, la obtención de los conjuntos de características de autenticación puede incluir obtener al menos dos conjuntos de características de modalidades diferentes; por ejemplo, datos de imagen y datos de audio. Además, en la etapa 643, la obtención de los conjuntos de características puede incluir obtener características de imagen a partir de datos de imágenes (por ejemplo, características SIFT, rasgos de la imagen, una profundidad de campo, etcétera), relacionadas con el objeto de autenticación válido en la representación digital. Todavía adicionalmente, la etapa 645 puede incluir calcular un valor *hash* como característica de autenticación a partir de la representación digital asociada a los objetos de autenticación válidos.

Debe apreciarse que los conjuntos de características de autenticación no representan necesariamente todas las posibles características asociadas a un objeto de autenticación válido. Por el contrario, las características de autenticación podrían representar simplemente las características asociadas a una parte del objeto; parte frontal, lateral, parte posterior, u otra parte. Por ejemplo, el conjunto de características de autenticación podría comprender datos de imagen de solamente una parte del objeto de autenticación. Así, la posición, orientación, encaramiento o cobertura de un solo objeto de autenticación puede influir en la activación del contenido. Las características de autenticación podrían incluir uno, dos, tres, siete o más tipos de datos de características. Los datos de características ilustrativos se podrían basar en datos de imagen, datos de movimiento, datos de audio, datos de

temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración, datos de rumbo u otros tipos de datos.

La etapa 650 incluye la obtención de una yuxtaposición entre los conjuntos de características de autenticación asociados a cada objeto de autenticación válido. La yuxtaposición puede considerarse un objeto construido o instanciado que incluye atributos de yuxtaposición que describen la posición, disposición, colocación relativa, u otra configuración de conjuntos de características dentro de un espacio de interacción. En un espacio físico tridimensional y en el que los conjuntos de características de autenticación incluyen características de datos de imagen (por ejemplo, características SIFT, puntos clave BRISK, coordenadas vSLAM, etcétera), los conjuntos de características podrían comprender conglomerados de características de imagen que presenten una extensión o posiciones dentro del espacio 3D. De este modo, la yuxtaposición puede incluir información referente a cómo están dispuestos múltiples conjuntos de características en el espacio 3D, uno con respecto a otro. Los atributos de yuxtaposición se pueden definir en términos de características individuales, conglomerados de características, o subconjuntos de características. Por ejemplo, si las características de autenticación comprenden múltiples conglomerados de características de imagen, la yuxtaposición se podría describir como una distancia geométrica en el espacio 3D entre el centroide del primer conglomerado y el centroide del segundo conglomerado. Debe apreciarse que el espacio de interacción puede ser un espacio multidimensional definido por más dimensiones que las dimensiones físicas. Las dimensiones adicionales de ejemplo pueden incluir tiempo, datos demográficos del usuario, intención o emoción derivada, relaciones sociales, u otras dimensiones.

Teniendo en cuenta que la yuxtaposición se puede describir con respecto a la disposición de los conjuntos de características de autenticación dentro de un espacio de interacción, debe apreciarse que la yuxtaposición puede incluir atributos obtenidos sobre la base de la colocación relativa en el espacio de interacción. Por lo tanto, la etapa 651 puede incluir la determinación de la yuxtaposición de los conjuntos de características de autenticación basándose en información de posición relativa, obtenida a partir de la posición relativa de los objetos de autenticación válidos correspondientes, dentro de la representación digital. La información de posición relativa también se podría determinar directamente a partir de los conjuntos de características de autenticación. La posición relativa puede ser una longitud física (por ejemplo, pulgadas, pies, millas, centímetros, metros, kilómetros, etcétera), una diferencia relativa entre escalas (por ejemplo, una escala emocional), u otra medida relativa dentro del espacio de interacción. De una manera similar, la etapa 653 puede incluir la determinación de la yuxtaposición de los conjuntos de características de autenticación sobre la base de información de orientación relativa de los correspondientes objetos de autenticación válidos en las representaciones digitales, o directamente a partir de la orientación relativa de los conjuntos de características de autenticación dentro del espacio de interacción. La información de orientación relativa puede incluir ángulos con respecto a un punto de referencia (por ejemplo, una cámara, un usuario, geolocalización, etcétera), o podría incluir orientaciones simples expresadas en términos de un encaramiento de los conjuntos de características (por ejemplo, hacia arriba, hacia abajo, a izquierda, a derecha, enfrentados, etcétera) uno con respecto a otro. Todavía adicionalmente, la etapa 655 puede incluir la determinación de la yuxtaposición sobre la base de información de tiempo relativa, con respecto a los conjuntos de características de autenticación. El tiempo relativo puede expresar cuándo aparece o cambia un primer conjunto de características con respecto a una existencia temporal de un segundo conjunto de características. La información de tiempo relativa también puede comprender información de movimiento (por ejemplo, trayecto aparente, velocidad, aceleración, sacudidas, etcétera), tiempo de aparición, tiempo de desaparición, tiempo de cambio (por ejemplo, rotación, cambio del encaramiento, migración de conjuntos de características, etcétera), migración o cambio de características en un conglomerado, u otra información relacionada con el tiempo.

Debe apreciarse que los conjuntos de características de autenticación, o los criterios desencadenantes del contenido, pueden depender de datos de geolocalización. Los datos de geolocalización pueden reflejar una localización de la interacción dentro de un edificio, o incluso fuera del edificio. Por ejemplo, los datos de localización se pueden obtener mediante GPS, o incluso técnicas que no sean GPS. Los ejemplos de técnicas que no son GPS incluyen el uso de un mapeo de base visual (por ejemplo, SLAM, vSLAM) con respecto a características visuales presentes en el entorno. Otro ejemplo de técnicas no GPS incluyen el uso de señales de satélites Iridium (por ejemplo, ráfagas QPSK de 20,32 mS, 1.626,104 MHz, etcétera), que son capaces de penetrar en edificios. Dicha información de geolocalización que no es GPS se puede incorporar a los atributos de yuxtaposición para la autenticación del usuario o la activación de contenido.

La etapa 660 puede incluir establecer, posiblemente por parte del agente de autenticación, un nivel de acceso a contenido en función de la yuxtaposición de los conjuntos de características de autenticación uno con respecto a otro. El nivel de acceso a contenido se puede determinar comparando los atributos de yuxtaposición con atributos vinculados a una política o conjunto de reglas que gobierna cómo debería accederse al contenido. Por ejemplo, una vez que el contenido se ha identificado como relevante, el mismo puede tener una política de acceso asociada, en la que la política indica criterios de nivel de acceso definidos en términos de atributos de yuxtaposición. La política puede estar vinculada directamente al contenido, o de manera independiente con respecto a este último. Como ejemplo (véase la Figura 5), el agente de autenticación se puede sumar a una base de datos de niveles de acceso, y puede usar los atributos de yuxtaposición para crear una consulta dirigida a la base de datos. Como respuesta a la consulta, la base de datos puede devolver niveles de acceso o una política con criterios que satisfagan la consulta.

La etapa 670 puede incluir activar el contenido, posiblemente por medio del agente de autenticación, basándose en los niveles de acceso al contenido. La activación puede producirse a través de diferentes técnicas. En algunas realizaciones, el contenido o partes del contenido pueden estar presentes *a priori* en el dispositivo de salida objetivo (por ejemplo, el dispositivo electrónico), y pueden darse instrucciones al dispositivo para que conceda acceso al contenido basándose en los niveles de acceso a contenido. En otras realizaciones, el contenido se puede activar iniciando una acción adicional mediante la provisión de órdenes o instrucciones al dispositivo de salida objetivo. La acción adicional podría incluir dar instrucciones a un dispositivo para que iniciase la descarga del contenido, efectuar una transacción financiera para comprar el contenido, lanzar un reproductor de contenido, lanzar una máquina virtual, u otras acciones.

La activación del contenido puede incluir activar el contenido en función de criterios desencadenantes de la activación, según se sugiere por medio de la etapa 675. Los criterios desencadenantes se pueden usar para dictaminar qué contenido está, de hecho, disponible basándose en el espacio de interacción. Por ejemplo, un contenido específico podría estar solamente disponible dentro de una geovalla definida o en un periodo de tiempo definido. Así, el contenido 1) puede hacerse disponible basándose en los criterios desencadenantes, y 2) puede controlarse basándose en niveles de acceso. Los criterios desencadenantes se pueden definir sobre la base de atributos o dimensiones del espacio de interacción. De este modo, los criterios desencadenantes de la activación pueden depender de tiempos absolutos o relativos, de una serie de solicitudes de autenticación u otros parámetros de autenticación, de la naturaleza de las características de autenticación (por ejemplo, imagen con respecto a sonido), otros factores diferentes a las características de autenticación (por ejemplo, contexto, geovallas, etcétera), factores excluyentes de características de autenticación (es decir, no dependen de las características de autenticación), u otros factores.

La etapa 680 incluye configurar un dispositivo de salida, posiblemente por parte del agente de autenticación, para presentar el contenido de acuerdo con los niveles de acceso a contenido. Tal como se ha mencionado anteriormente, el dispositivo de salida se puede configurar a través del envío de una o más órdenes al dispositivo de salida para realizar una acción. Las órdenes que configuran el dispositivo, o sus reproductores de contenido asociados, dependen de la naturaleza del contenido. Por ejemplo, cuando el contenido comprende un archivo de medios (por ejemplo, vídeo, música, etcétera), las órdenes podrían impedir o permitir que el reproductor correspondiente en el dispositivo de salida desplace en el tiempo el contenido basándose en los niveles de acceso concedidos. No obstante, si el contenido comprende un archivo de impresora 3D, las órdenes podrían impedir o permitir que la impresora crease un objeto 3D a partir del archivo en color.

En algunas realizaciones, la configuración del dispositivo de salida puede incluir dar instrucciones al dispositivo de salida para lanzar una máquina virtual según se sugiere mediante la etapa 681. La máquina virtual podría incluir una máquina virtual Java®, una máquina virtual .NET®, una máquina virtual Phyton, una máquina virtual VMWare®, u otra máquina virtual. El uso de una máquina virtual se considera ventajoso ya que el contenido se puede aislar del usuario basándose en el nivel de acceso. Por ejemplo, la máquina virtual se puede lanzar y el contenido se puede almacenar en una memoria protegida (por ejemplo, memoria cifrada, contenedor protegido, FIPS-140, etcétera). El método puede incluir además la etapa 683, que protege la máquina virtual con respecto a derechos de contenido de acuerdo con los niveles de acceso. A continuación, el controlador (por ejemplo, el proveedor de contenido) de la máquina virtual puede permitir al usuario que observe el contenido al mismo tiempo que garantiza que el controlador limite el acceso. Un reproductor de contenido, o un contenido dentro de la máquina virtual, se puede proteger bloqueando el contenido o reproductor por medio de un token de seguridad, cifrando el contenido, o aplicando otras medidas de seguridad. Además, la etapa 685 puede incluir la restricción, por parte de la máquina virtual, del acceso al contenido de acuerdo con los niveles de acceso. Tal como se ha mencionado previamente, puede ordenarse a la máquina virtual que bloquee las características de un reproductor de contenido o de un dispositivo de salida, con respecto a la presentación del contenido.

Ejemplos

Las siguientes secciones describen varias realizaciones de la materia objeto de la invención.

Activación de contenido basada en objetos de autenticación

Un aspecto de la materia objeto de la invención incluye la activación de contenido basada en objetos de autenticación, incluyendo métodos de activación de contenido. Los métodos pueden incluir una etapa para proporcionar acceso a un agente de autenticación configurado para autenticar un usuario, dispositivo, u otra entidad con respecto a contenido deseable. El acceso se puede proporcionar por medio de una interfaz de dispositivo electrónica, posiblemente mediante una conexión de Internet a un teléfono celular. En algunas realizaciones, el agente de autenticación, posiblemente junto con otros elementos del ecosistema, se puede ofrecer como un servicio de tarificación independiente a los proveedores de contenido o a los consumidores.

El método puede incluir la etapa de obtención de una representación digital multi-modal de una interacción con por lo menos un objeto físico. La representación digital multi-modal puede incluir varios tipos de datos según se ha descrito previamente, y puede reflejar la interacción de una entidad con una escena o el objeto físico. Debe apreciarse que la representación digital comprende datos del dispositivo electrónico u otras fuentes de datos. Las

interacciones pueden incluir tomar una imagen del objeto físico, estar cerca del objeto físico, interaccionar físicamente con el objeto, monitorizar el objeto físico, u otros tipos de interacciones, directas o indirectas. Las modalidades de ejemplo en una representación digital multi-modal pueden incluir uno, dos o más de los siguientes tipos de datos, datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración, datos de velocidad, datos de rumbo, cambios en unos datos basales, u otros tipos de datos.

Tal como se ha descrito previamente, el objeto físico puede incluir prácticamente cualquier tipo de objeto, ya que los algoritmos usados para analizar la representación digital pueden ser indiferentes al propio objeto. Más bien, los algoritmos buscan características que se encuentran en los datos asociados (por ejemplo, características SIFT, características de audio, firmas de datos de sensores, etcétera). El objeto físico puede incluir diferentes tipos de objetos, incluyendo soportes impresos, objetos sustancialmente tridimensionales, o incluso dispositivos informáticos que tienen imágenes representadas. Los medios impresos ilustrativos podrían incluir un permiso de conducir, una firma, un cartel, una valla publicitaria, una fotografía, una imagen representada, un libro, un periódico, o una revista. Los objetos tridimensionales de ejemplo que se pueden usar como base para la autenticación incluyen una persona, una cara, un animal, un vehículo, un edificio, un juguete, una planta, un dispositivo informático, una construcción, una figurita, u otros objetos. Las imágenes representadas ilustrativas podrían incluir una pantalla de ordenador, un quiosco interactivo, un tablón de anuncios electrónico, un televisor, una pantalla de cine, un sistema de juego, u otros tipos de imágenes representadas.

Las características de autenticación también pueden comprender diferentes modalidades sobre la base de las modalidades de la representación digital. Cada tipo de modalidad se puede tratar por separado o conjuntamente para crear un esquema de autenticación más sofisticado o complejo. En realizaciones más preferidas, las características de autenticación incluyen por lo menos dos modalidades diferentes, por ejemplo datos de imagen y datos de audio. Una característica de autenticación especialmente contemplada incluye datos de imágenes asociados a un objeto de autenticación o a por lo menos una parte del objeto de autenticación. En algunas realizaciones, la característica de autenticación puede incluir un valor *hash*, posiblemente un valor *hash* perceptual, de la imagen.

El método incluye además reconocer el objeto físico con respecto a otros objetos asociados a la interacción, donde el objeto físico se identifica como un objeto de autenticación válido. El objeto físico se puede identificar basándose en información obtenida a partir de la representación digital multi-modal, que incluye características de objetos. El objeto físico se puede reconocer mediante búsquedas en una base de datos de objetos de autenticación que tiene objetos de autenticación con características de objeto similares a aquellas obtenidas a partir de la representación digital.

El método puede incluir además obtener una pluralidad de características de autenticación relacionadas con el objeto de autenticación, donde las características de autenticación pueden ser valores o parámetros cuantificados de consideración, para llevar a cabo la autenticación. Por ejemplo, las características de autenticación pueden ser claves de consideración, que incluyen posiblemente características SIFT, características de audio, valores *hash*, rasgos de imagen o de datos de imagen, información de profundidad de campo de la imagen o audio, u otros tipos de datos que se pueden obtener a partir de la representación digital o información asociada al objeto de autenticación.

Debe apreciarse que la interacción con el objeto físico y la representación digital resultante puede comprender interacciones con múltiples objetos de autenticación tal como se ilustra en la Figura 1. En escenarios en los que múltiples objetos de una escena se consideran objetos de autenticación, las características de autenticación pueden obtenerse a partir de la yuxtaposición o disposición de los objetos uno con respecto a otro. Las características de autenticación podrían incluir información de posición relativa asociada a la disposición de los objetos físicos, o podrían incluir información de orientación relativa asociada a los objetos físicos. Por ejemplo, si los objetos de autenticación incluyen un permiso de conducir y una taza de café, la orientación del asa de la taza con respecto al permiso de conducir podría indicar un nivel de acceso deseado. Si el asa apunta desviada con respecto al permiso de conducir, tal vez podría activarse un contenido mínimo. Si el asa apunta al permiso, tal vez podría activarse el contenido completo.

La autenticación puede requerir la presencia satisfactoria, o incluso la ausencia, de una o más características de autenticación antes de que pueda activarse el contenido. En algunos escenarios, el agente de autenticación puede requerir por lo menos tres características de autenticación, o incluso hasta siete o más características de autenticación. Considérese un escenario de atención sanitaria en el que un paciente ha entrado en una sala de urgencias. Un doctor puede tomar una imagen del paciente (es decir, un objeto 3D del mundo real), pronuncia el nombre del paciente, y pronuncia el nombre del doctor hacia un ordenador de tipo tableta. Una plataforma de reconocimiento analiza los datos de imagen y de audio (por ejemplo, representación digital de una interacción multi-modal) para obtener características asociadas al paciente y la voz. Además, la representación digital de la tableta puede incluir una localización GPS, un tiempo, u otra información. A continuación, las características obtenidas se usan para identificar uno o más objetos de autenticación, de manera que, en este escenario, un objeto de autenticación puede incluir la cara del paciente. Como respuesta, un agente de autenticación obtiene un conjunto de

características de autenticación a partir de la representación digital, así como información a partir de la información del objeto de autenticación. Las características de autenticación podrían incluir (a) características SIFT de la cara del paciente, (b) patrón vocal del doctor, (c) el nombre del paciente, (d) el nombre del doctor, (e) las coordenadas GPS de la sala de urgencias, (f) un tiempo, (g) profundidad de campo de la cara de la persona, o (h) posiblemente una imagen del permiso de conducir o de la tarjeta sanitaria del paciente. Así, puede usar un gran número de características de autenticación para determinar un nivel de acceso a contenido. En este ejemplo, el nivel de acceso a contenido podría permitir que el doctor accediese a todos los historiales médicos electrónicos del paciente debido a una situación de urgencias.

Sobre la base de las características de autenticación, el método también puede incluir establecer un nivel de acceso a contenido. El nivel de acceso a contenido indica cuál de los contenidos, qué contenido, o en qué medida se hace que esté disponible el contenido para un consumidor del mismo. El contenido puede abarcar un amplio espectro de tipos de medios o información incluyendo información de transacciones, información de entretenimiento, información de noticias, información deportiva, información promocional, información médica, información de seguridad, información de juegos, aplicaciones o instrucciones de software, información didáctica, u otros tipos de datos.

Un tipo especialmente preferido de contenido incluye información promocional relacionada con bienes, servicios, u otros tipos de productos. Por ejemplo, el objeto físico podría ser un objeto que se puede comprar en un supermercado. El propio producto podría ser un objeto de autenticación, y la información promocional podría incluir un cupón a aplicar en la compra del producto, un mensaje publicitario, un anuncio, u otro tipo de información promocional.

El método incluye también activar el contenido de acuerdo con el nivel de acceso. La activación puede producirse en el agente de autenticación o puede incluir la provisión de los niveles de acceso a un servidor de contenido, el cual, a su vez, activa el contenido. En algunas realizaciones, deben cumplirse criterios desencadenantes de la activación, adicionales, antes de que pueda producirse la misma. Por ejemplo, los criterios desencadenantes de la activación podrían requerir la entrada de un número de solicitudes de autenticación al sistema o un tiempo absoluto. Tal vez un episodio de una historia interactiva se activa únicamente cuando cien usuarios capturan una imagen de un cartel de la película. Otros ejemplos de criterios desencadenantes incluyen factores diferentes a los criterios de autenticación, o incluso excluyentes de los criterios de autenticación. Por ejemplo, los criterios de autenticación podrían depender de una hora específica del día o de una alerta de noticias.

Los métodos contemplados incluyen además configurar un dispositivo electrónico, un teléfono celular u ordenador de tipo tableta, por ejemplo, para presentar el contenido de acuerdo con los niveles de acceso. Tal como se ha descrito previamente, la configuración de un dispositivo electrónico para presentar o reproducir el contenido puede incluir dar instrucciones al dispositivo electrónico para lanzar una máquina virtual, preferentemente una máquina virtual protegida, bajo el control del servidor de contenido o de un proveedor de contenidos. La máquina virtual puede restringir el acceso al contenido basándose en los niveles de acceso. Los dispositivos electrónicos ilustrativos que pueden beneficiarse de dicho contenido incluyen un teléfono celular, un ordenador de tipo tableta, un ordenador convencional, un vehículo, un quiosco interactivo, una máquina expendedora, un robot, un electrodoméstico, un dispositivo médico, un sistema de seguridad, una consola de juegos, u otros tipos de dispositivo.

Los algoritmos usados para analizar la representación digital de la interacción multi-modal buscan características asociadas a los objetos que participan en las interacciones o características en los datos. Dichas características no incluyen o requieren necesariamente la descodificación de símbolos en una imagen. Así, las características de autenticación pueden carecer de información obtenida a partir de etiquetas simbólicas, por ejemplo un código de barras, asociadas en el objeto de la interacción. Sin embargo, el uso de información simbólica descodificada (por ejemplo, caracteres, números, códigos de barra, etcétera) puede potenciar el proceso.

Autenticación basada en el reconocimiento de un objeto como objeto de autenticación

Otro aspecto de la materia objeto de la invención se considera que incluye sistemas de distribución de contenido, donde se activa contenido basándose en el reconocimiento de que un objeto real es, de hecho, un objeto de autenticación. Los sistemas de distribución pueden incluir una base de datos de objetos de autenticación, una plataforma de reconocimiento, y un agente de autenticación, tal como se ilustra en la Figura 1. La siguiente descripción profundiza en el ecosistema de la Figura 1.

La base de datos de objetos de autenticación almacena elementos de autenticación, donde los elementos están vinculados a usuarios específicos y tienen también un conjunto de características de autenticación válidas referentes al objeto. Las características de autenticación válidas pueden representar características requeridas y valores asociados o características condicionales. Además, los elementos de autenticación pueden incluir punteros o referencias al contenido que sería desbloqueado por las características de autenticación cuando la presencia o ausencia de las características en una interacción presente propiedades adecuadas. En algunas realizaciones, la base de datos de objetos de autenticación puede comprender una base de datos de imágenes o un motor de búsqueda de imágenes que almacene miles, millones, o un número mayor de imágenes que representan objetos de autenticación. Las bases de datos de imagen ilustrativas que se podrían adaptar adecuadamente para su uso con la materia objeto de la invención incluyen imágenes de Google®, TinEye Reverse Image Search Engine™, (véase el

URL www.tineye.com), bases de datos de imágenes médicas, u otros tipos de bases de datos de imágenes. En algunas realizaciones, las imágenes se indexan según características relevantes de autenticación de imágenes (por ejemplo, SIFT, profundidad de campo, rasgos de datos de imágenes, metadatos, etcétera).

La plataforma de reconocimiento se puede configurar para procesar específicamente datos de imagen asociados a la representación digital junto con otros tipos de modalidades. Una vez que la plataforma de reconocimiento obtiene los datos de imagen, la misma puede obtener características de objetos referentes a los objetos de la imagen. Preferentemente, la plataforma de reconocimiento usa las características de los objetos para diferenciar o reconocer objetos de la imagen, con respecto a otros objetos, en donde los objetos reconocidos se consideran como objetos de autenticación. La plataforma de reconocimiento puede presentar las características del objeto ante la base de datos de objetos de autenticación para comparar las características del objeto con la correspondiente o las correspondientes de las características de autenticación válidas, con el fin de determinar si los objetos representados visualmente son en realidad objetos de autenticación. Podría devolverse más de un elemento de autenticación. En un escenario de este tipo, el conjunto de resultados se puede clasificar de acuerdo con cómo de bien se ajustaron las características de objeto al conjunto de características de autenticación válidas de cada elemento.

El agente de autenticación usa las características de objetos, incluyendo las características de imágenes, y las características de autenticación válidas, para determinar un nivel de acceso a contenido según se ha descrito previamente. El agente de autenticación puede determinar el nivel de acceso a contenido basándose en punteros o referencias en los elementos de autenticación correspondientes, o basándose en una solicitud realizada por el usuario. En algunas realizaciones, un usuario podría solicitar contenido específico en el que objetos de contenido en una base de datos de contenido apuntan a elementos de autenticación requeridos. Por contraposición, en otras realizaciones, los elementos de autenticación apuntan a contenido que puede ser activado por el elemento de autenticación. Una vez que el agente de autenticación ha establecido los niveles de acceso al contenido, el agente de autenticación puede autorizar a un servidor de contenido a que active el contenido para el usuario.

Información de productos a partir de un flujo continuo de vídeo capturado

Todavía otro aspecto de la materia objeto de la invención incluye métodos de obtención de información de productos. Los métodos representan una realización específica en la que consumidores de contenido pueden activar información de productos, basándose en la captura de una imagen de un cuadro de vídeo en un flujo continuo de vídeo. Los métodos incluyen proporcionar acceso a un servidor de reconocimiento u otro tipo de plataforma de reconocimiento. El servidor de reconocimiento puede funcionar como un servicio, un motor de búsqueda por ejemplo, donde los consumidores pueden presentar una o más imágenes al servicio a través de una conexión en red.

El servidor de reconocimiento obtiene un cuadro de vídeo capturado a partir de un flujo continuo de vídeo visualizado, en donde el cuadro de vídeo se transmite desde un dispositivo electrónico (por ejemplo, teléfono celular, vehículo, cámara, ordenador de tipo tableta, etcétera). Debe apreciarse que la expresión “cuadro de vídeo capturado” se usa como eufemismo para significar al menos una imagen fija de flujo continuo de vídeo. El cuadro de vídeo capturado podría ser uno o más cuadros concretos del flujo continuo de vídeo, capturados posiblemente durante la reproducción en el dispositivo electrónico. Adicionalmente, el cuadro de vídeo capturado puede incluir una imagen fija tomada por un sensor de cámara en un dispositivo electrónico, o podría incluir una imagen fija en la que dos o más cuadros de vídeo concretos cambian del uno al otro, lo cual podría dar como resultado una imagen algo borrosa. El servidor de reconocimiento puede obtener el cuadro de vídeo capturado a partir de un conjunto electrónico a través de una conexión en red. El dispositivo electrónico ilustrativo que se podría usar para capturar el cuadro de vídeo capturado incluye un teléfono celular, un sistema de juego, un ordenador, un ordenador de tipo tableta, un quiosco interactivo, una valla publicitaria electrónica, o cualquier tipo de dispositivo que esté configurado con una cámara.

Con independencia de la naturaleza del cuadro de vídeo capturado, el servidor de reconocimiento obtiene una o más características de cuadro del cuadro de vídeo capturado. Las características de cuadro pueden incluir características SIFT, valores *hash* perceptuales, histogramas, objetos reconocidos, u otras características que se pueden obtener a partir del cuadro de vídeo capturado, según se ha descrito previamente.

El servidor de reconocimiento puede usar las características de cuadro para identificar un flujo continuo de vídeo conocido que tenga características similares. Por ejemplo, el servidor de reconocimiento puede presentar las características de cuadro como consulta ante una base de datos de flujos continuos de vídeo conocidos. Como respuesta, la base de datos de flujos continuos de vídeo devuelve un conjunto de resultados que tiene uno o más flujos continuos de vídeo conocidos que han sido analizados *a priori,* posiblemente cuadro a cuadro. Los vídeos del conjunto de resultados se pueden clasificar de acuerdo con una o más de las características de cuadro obtenidas. Además, el conjunto de resultados puede incluir información adicional sobre los flujos continuos de vídeo originales incluyendo información asociada de productos. Por ejemplo, un individuo podría presentar una captura de pantalla de un programa de televisión y presentarla ante el servidor de reconocimiento. El servidor de reconocimiento puede identificar el programa de televisión original, y devolver un listado de productos mencionados en el programa o mencionados en anuncios durante la representación del programa.

Los métodos contemplados incluyen además la configuración de un dispositivo electrónico para presentar la información de producto al consumidor. La información del producto, o, para el caso, otros tipos de información, puede incluir un nombre, una marca, un número de modelo, un precio de compra, instrucciones que configuran el dispositivo para involucrarse en una transacción, u otros tipos de información.

En algunas realizaciones, los flujos continuos de vídeo también pueden comprender datos de audio que se pueden capturar junto con el cuadro de vídeo capturado. Cuando se captura el cuadro de vídeo capturado, también pueden capturarse los datos de audio asociados al cuadro. El servidor de reconocimiento también puede obtener características de audio, las cuales se pueden usar también para identificar flujos continuos de vídeo, o incluso posiciones en el flujo continuo de vídeo.

En realizaciones especialmente preferidas, los datos de audio pueden comprender datos representativos de sonidos fuera del alcance del oído humano; por ejemplo, una firma de ultrasonidos. Así, un flujo continuo de vídeo puede incluir información de audio adicional que se puede usar para identificar el flujo continuo de origen, productos, una emisión de radiodifusión, una fuente, u otro objeto. En una realización del tipo mencionado, el servidor de reconocimiento puede analizar el flujo continuo de audio para obtener componentes de frecuencia que se pueden utilizar para reconocer el flujo continuo o producto asociado al flujo continuo.

Casos prácticos

La siguiente descripción presenta escenarios de casos prácticos específicos, destinados a clarificar adicionalmente la materia objeto de la invención con respecto a mercados específicos. Debe apreciarse que cada escenario de un caso práctico se considera también como materia objeto de la invención.

Uno de los casos prácticos incluye la provisión de programas televisados basados en información de productos. Cuando el consumidor ve un producto interesante, u otro objeto en un programa televisado, el consumidor puede adquirir una captura de la pantalla usando su teléfono celular. Además, el programa puede comprender una o más señales de alta frecuencia incorporadas, sonidos por encima de 20 KHz, las cuales pueden transportar información adicional que identifica aspectos del programa o productos del programa. Por ejemplo, el teléfono celular puede capturar las señales de audio de alta frecuencia, y descodificar las señales para obtener la información incorporada. Debe apreciarse que el teléfono celular puede funcionar como plataforma de reconocimiento según se desee. Por lo tanto, el teléfono celular puede enviar los datos sin procesar o características obtenidas de la imagen o audio, a un servicio de autenticación, el cual activa información de productos asociada a la pantalla de vídeo. Por ejemplo, un vídeo musical podría mostrar diversas tendencias de moda. El usuario del teléfono celular puede comprar productos de esas tendencias solicitando información del producto asociada al vídeo.

Otro de los casos prácticos puede incluir la activación de contenido asociado a una publicación o cartel. Considérese un escenario en el que un consumidor recibe una revista que tiene una o más fotografías de un acontecimiento deportivo. El consumidor usa su teléfono celular para capturar una imagen de la fotografía. La imagen de la fotografía se puede autenticar con respecto a una base de datos de imágenes, tal vez sobre la base de imágenes disponibles en Gettyimages® (véase el URL www.gettyimages.com). La imagen se analiza y compara con imágenes conocidas. Si se encuentra una coincidencia, entonces puede enviarse al teléfono celular del consumidor una señal de vídeo suministrada concreta, en vivo o grabada, del acontecimiento deportivo concreto.

Un caso práctico similar incluye la activación de contenido sobre la base de imágenes correspondientes a un cartel o valla publicitaria. Considérese una valla publicitaria o cartel de promoción que anuncia un acontecimiento próximo desconocido. El objetivo es desarrollar un caldo de cultivo o interés viral en el acontecimiento misterioso, quizás el estreno de una película o el lanzamiento de un nuevo tipo de teléfono inteligente. Tal vez, la promoción simplemente menciona un día y una hora, y a continuación dice que el contenido se activará si 10.000 personas solicitan su activación al mismo tiempo sobre la base de una imagen capturada de la promoción. Cuando llega el día y la hora, y entran 10.000 solicitudes, se activa el contenido. Debe apreciarse que las imágenes de la promoción comprenden características de activación, mientras que las 10.000 solicitudes representan criterios desencadenantes de la activación.

Todavía adicionalmente, un cartel podría representar un canal de radiodifusión trans-media. Una imagen del cartel puede activar contenido actual que se esté radiodifundiendo para todos los espectadores del cartel. El contenido también se puede sincronizar, de manera que todos los consumidores vean o reciban el mismo contenido sustancialmente al mismo tiempo. Por ejemplo, un cartel de Kobe Bryant puede proporcionar contenido actualizado de una manera diaria, o incluso durante todo el día. Cuando el consumidor activa el contenido capturando una imagen del cartel, el consumidor recibiría el contenido que se está distribuyendo en ese momento de manera similar a una emisora de radio o un canal de televisión. El contenido podría incluir programación basada en titulares deportivos, noticias, mensajes de blogs, segmentos de vídeo, comentarios, un partido real, u otros tipos de contenido.

Todavía otro caso práctico incluye proporcionar cupones a consumidores mientras están realizando compras. Cuando el consumidor está en la tienda, el mismo puede capturar imágenes de productos objetivo, posiblemente en un intento de efectuar una comparación de precios. No obstante, podría ser que la tienda no desease perder el

consumidor. Como respuesta, la tienda que funciona como servicio de contenidos podría detectar el evento de comparación de precios sobre la base de información de la localización, características de imagen, u otros factores. El evento de comparación de precios podría ser detectado por un motor de búsqueda remoto que notifica a la tienda, o podría ser detectado dentro de la tienda en el caso de que el teléfono celular del consumidor utilice el punto de acceso Wi-Fi de la tienda. Con independencia de cómo se detecte el evento, la tienda puede activar cupones asociados al producto en un intento de conservar el consumidor. Por lo tanto, el minorista puede proporcionar cupones como una forma de contenido activado, sin tener que modificar el inventario o etiquetar productos existentes expuestos, con códigos de barras.

Todavía otro caso práctico puede incluir juegos basados en ordenador. La infraestructura dada a conocer permite la creación de una capa de contenido bajo demanda sobre el mundo real, donde el contenido se puede activar basándose en una o más interacciones de jugadores con el mundo real. Por ejemplo, podría activarse contenido sobre la base de las interacciones de múltiples jugadores del juego, por contraposición a las interacciones de un solo jugador. Un escenario de este tipo crea un juego capaz de soportar “magia”, “hechizos”, o física alternativa. Tal vez en un juego de realidad aumentada basado en un escenario de fantasía, los jugadores de un equipo podrían tener que estar, todos ellos, en una localización específica, e interaccionar con los objetos de esa localización. En algunos casos, los jugadores podrían tener que actuar al unísono para simular un ritual, o actuar por separado para simular que se están apoyando mutuamente en una batalla. Si los jugadores logran capturar una o más representaciones digitales de sus interacciones, donde las representaciones digitales tienen las características de autenticación o criterios desencadenantes apropiados, los jugadores activarían un contenido nuevo. Las capacidades ofrecidas por Fourth Wall Studios™ (véase el URL fourthwallstudios.com) se podrían adaptar adecuadamente para su uso en un escenario de juegos del tipo mencionado.

Existen también casos prácticos asociados a la asistencia sanitaria. Uno de los ejemplos incluye el uso de información genómica para activar contenido. Por ejemplo, puede analizarse el genoma de un individuo (por ejemplo, humano, mascota, animal, planta, etcétera) para determinar características del genoma de la persona. Las técnicas ilustrativas para obtener las características genómicas incluyen aquellas desarrolladas por Five3 Genomics™. A continuación, las características genómicas se pueden vincular con una firma generada o una imagen de un mapa de calor del genoma. La firma o mapa de calor se puede considerar un código de barras o código QR representativo del genoma. Además, las características de la firma se convierten en las características de autenticación del genoma. A continuación, la firma puede ser un objeto de autenticación accesible al público, que se puede usar para activar el contenido. La seguridad del contenido se puede potenciar adicionalmente requiriendo modalidades adicionales más allá de la captura de una imagen de la firma, que incluyen posiblemente datos de localización, datos de posición, datos de objetos 3D, datos de voz, u otros factores.

Otra de las aplicaciones sanitarias podría incluir la activación de contenido basada en una situación de urgencias tal como se ha descrito previamente. Quizás un doctor en una sala de urgencias toma una imagen de una persona para activar sus historiales médicos, o toma una imagen de la firma genómica de una persona o del mapa de calor en la parte posterior de su permiso de conducir o tarjeta sanitaria. Tras una autenticación correcta, los historiales médicos del paciente se activan para el doctor.

Aún todavía otro de los casos prácticos puede incluir un sistema de identificación para mascotas. Los propietarios de mascotas pueden registrar sus mascotas en un servicio en línea que ofrece las capacidades descritas en este documento. El propietario puede presentar una o más fotografías de su mascota como objetos de autenticación. El sistema puede obtener características de autenticación a partir de las fotografías, u ofrecer al propietario de la mascota una opción para seleccionar características de autenticación deseadas. El propietario de la mascota puede poner una imagen de su mascota en el collar de esta última para facilitar la identificación. Cuando la mascota se pierde, una persona que la encuentra puede tomar una imagen de ella o de la fotografía que está en el collar. A continuación, las características obtenidas a partir de la imagen se pueden usar para activar contenido. En este caso específico, el contenido activado podría incluir la información de contacto al propietario, la cual se puede presentar a la persona que encontró la mascota. Contenido adicional podría incluir identificación del propietario, tal vez un vídeo o una imagen del propietario con la mascota, que se puede enviar a la persona que la encontró. Además, el sistema puede activar contenido en el teléfono celular del propietario, indicando dónde se localiza la persona que encontró la mascota o incluso indicaciones sobre cómo encontrar la mascota.

Consideraciones adicionales

Las siguientes consideraciones adicionales se presentan para ilustrar todavía más la naturaleza variada de la materia objeto de la invención.

Debe apreciarse que la materia en cuestión se presenta en términos de un ecosistema de autenticación y de activación de contenido. Cada elemento del ecosistema se presenta como un elemento funcional diferenciado en el sistema, y en comunicación mutua con otros. No obstante, los elementos del sistema pueden estar integrados en un solo dispositivo (por ejemplo, un teléfono celular) o pueden estar distribuidos por múltiples dispositivos (por ejemplo, un teléfono celular, un televisor, y un sistema informático basado en la nube), según se desee. Se contempla específicamente que los dispositivos electrónicos pueden comprender la plataforma de reconocimiento, o aspectos de la plataforma de reconocimiento.

Puede accederse a contenido activado de diferentes maneras. En algunas realizaciones, el contenido simplemente se puede distribuir al dispositivo electrónico una vez que se ha alcanzado la autenticación correcta y se determinan los niveles de acceso al contenido. El contenido se puede enviar sin solicitud previa desde un servidor de contenido, o se puede enviar desde el dispositivo tras solicitud previa. Así, cada individuo que recibe el contenido recibe el contenido individualmente sobre la base de sus propias interacciones y en momentos diferentes. En otras realizaciones, se puede distribuir contenido entre múltiples individuos de una manera sincronizada, donde los individuos reciben el mismo contenido sustancialmente al mismo tiempo. Por ejemplo, haciendo referencia nuevamente al cartel del ejemplo de Kobe Bryant, cada individuo podría recibir contenido de radiodifusión al mismo tiempo. Todavía otras circunstancias podrían incluir la distribución del contenido activado sincronizado para solamente unos cuantos seleccionados que hayan satisfecho de manera exitosa los criterios desencadenantes de la activación, y que hayan encontrado características de activación pertinentes.

Otra de las consideraciones se refiere al número de consumidores que están viendo contenido activado, al mismo tiempo. Si muchos miles, cuando no millones o incluso miles de millones, de personas activan contenido al mismo tiempo, la infraestructura debe soportar la distribución del contenido a un número enorme de individuos. El contenido se puede almacenar temporalmente en zonas periféricas (*edged-cached*) antes de su activación, de manera que esté fácilmente disponible para la distribución final. El contenido se puede almacenar temporalmente en la periferia en conmutadores de red, en servidores intermediarios, en dispositivos o reproductores de redes de área personal, en proveedores de servicios de internet, en puntos de acceso, u otros lugares que tengan memoria suficiente para el contenido. Por ejemplo, historiales médicos o contenido genómico se podrían almacenar temporalmente en muchos de los servidores del National Lambda Rail (véase www.nlr.net).

La activación de contenido para muchos miles de personas aporta también oportunidades para los proveedores de contenido. Se puede realizar un seguimiento de las interacciones entre consumidores y el ecosistema contemplado, con fines de elaborar índices, donde literalmente miles de individuos activan contenido al mismo tiempo. Los datos demográficos de los individuos se pueden obtener basándose en la información de su cuenta, sujeta a restricciones de privacidad, y proporcionada a los proveedores de contenido.

Debido al carácter de la infinidad de posibles características de autenticación o modalidades de autenticación, los proveedores y consumidores de contenido tienen acceso a muchas formas posibles de crear requisitos de autenticación. Un espectro tan amplio de posibilidades da origen a la capacidad de crear un sentido de capacidad de negación plausible. Por ejemplo, si una persona se ve forzada a desvelar sus factores de autenticación, ésta podría revelar únicamente un pequeño aspecto de sus factores, el cual descubre únicamente un contenido mínimo. Considérese un escenario en el que las características de autenticación requieren que el bolígrafo de una persona con un clip se sitúe en yuxtaposición con su anillo de boda. Cuando el clip del bolígrafo está encarado al anillo de boda, puede activarse el contenido completo de la persona. No obstante, si el clip está alejado del anillo de boda, lo cual es un cambio muy pequeño, se activa solamente una información mínima. Por lo tanto, la persona parece haber dado a conocer información de una manera tal que puede negar de forma plausible la existencia de cualquier información adicional. Todavía adicionalmente, la colocación del bolígrafo y el anillo en otras orientaciones podría activar contenido en otros dispositivos electrónicos. Tal vez la colocación del anillo en la punta del bolígrafo podría activar contenido que incluye un mensaje de texto o un mensaje telefónico para una comisaría.

Realizaciones especialmente preferidas integran en un sistema operativo aspectos, funciones o responsabilidades del ecosistema de distribución de contenido y de autenticación multi-modal. Un planteamiento de este tipo supone un alivio para el usuario de un dispositivo electrónico en cuanto a descarga de una aplicación dedicada, la instalación de software nuevo, o la interacción con el dispositivo de una manera compleja. Por ejemplo, a medida que el dispositivo electrónico recoge datos ambientales, un módulo de reconocimiento puede analizar los datos ambientales u otra representación digital que fluya hacia el dispositivo, para reconocer objetos o características que podrían ser relevantes para el entorno en el que se encuentra el propio dispositivo electrónico. Si fuera necesario o deseable, el sistema operativo puede descargar su análisis hacia servicios distantes. Además, el sistema operativo puede instanciar una o más máquinas virtuales para presentar contenido relevante, incluyendo posiblemente software de ejecución, donde las máquinas virtuales permanecen bajo el control del sistema operativo o proveedores de contenido remotos.

Según se ha hecho referencia muy anteriormente en este documento, el contenido puede adoptar muchas formas diferentes. Una forma especialmente contemplada de contenido incluye instrucciones ejecutables que configuran el dispositivo electrónico objetivo para que entre en acción. Por ejemplo, un consumidor podría formar una imagen de un cartel de una película con su sistema de juego de mano, equipado con una cámara. Tras la autenticación correcta, un proveedor de la película puede dar instrucciones al sistema de juego para que lance una máquina virtual acoplada con un sistema de transacción. La máquina virtual se puede cargar con instrucciones que configuren el sistema de juego para presentar una interfaz de compra. Si el usuario compra la película, esta se puede activar en la máquina virtual de una manera segura. Las transacciones representan solamente un tipo de acción que puede realizarse como respuesta a la recepción de una instrucción de contenido. Se contemplan todos los tipos de acciones.

La presentación de contenido puede comprender más que la representación de imágenes en un dispositivo electrónico, la reproducción de música, o la configuración del dispositivo electrónico para iniciar una acción. En

algunas realizaciones, la presentación de contenido puede incluir la construcción o la creación de objetos tridimensionales. Por ejemplo, el contenido puede incluir instrucciones para una impresora 3D con capacidad de construir un objeto 3D a partir de resina, plástico, polvo, u otros materiales. Impresoras 3D de ejemplo que podrían adaptarse adecuadamente para su uso con la materia objeto de la invención incluyen MakerBot™ (véase www.makerbot.com), máquinas CNC, ZPrinter® (véase www.zcorp.com), u otros dispositivos electrónicos capaces de generar un objeto tridimensional. Debe apreciarse que se considera que la materia objeto de la invención incluye la instanciación de una máquina virtual dentro de una impresora 3D o una máquina CNC bajo el control de una fuente externa, de manera que la impresora pueda generar un objeto aunque conservando los derechos del proveedor de contenidos.

Se considera también que la materia objeto de la invención incluye el registro de una disposición de objetos de autenticación válidos, y posiblemente la vinculación de la disposición con una o más interacciones. El registro de objetos de autenticación válidos puede producirse a través de una o más técnicas. Una de las técnicas posibles incluye la disposición de objetos de autenticación válidos (por ejemplo, un permiso de conducir, un juguete, un zapato, gestos, palabras pronunciadas, etcétera) dentro del espacio de interacción, y la grabación del acto de disponer los objetos en conjunto como una representación digital de la interacción. Un agente de autenticación puede analizar la representación digital para compilar conjuntos de características de autenticación relacionados en una yuxtaposición, la cual, a su vez, se puede almacenar dentro de la base de datos de autenticación. A continuación, la entidad que crea la disposición puede vincular la yuxtaposición con contenido o acciones deseados (por ejemplo, lanzamiento de una aplicación, ejecución de una transacción, envío de un mensaje, etcétera). Otra técnica podría incluir la captura de representaciones digitales de cada objeto de autenticación válido individualmente, y el registro de cada uno de los objetos individuales. A continuación, se capturan una o más yuxtaposiciones de los objetos individuales en relación mutua, donde cada yuxtaposición se puede enlazar con contenido. Considérese como ejemplo un sistema de seguridad de un dispositivo inteligente (por ejemplo, teléfono celular, tableta, tabletófono, ordenador, quiosco interactivo, ATM, etcétera). Un usuario podría bloquear el acceso al dispositivo registrando múltiples objetos con el uso de diferentes modalidades de captura de datos. Quizás el usuario podría bloquear el dispositivo al requerir una yuxtaposición entre su anillo de boda, palabras pronunciadas, y el movimiento del anillo de boda cruzando una imagen de fondo. Una vez registrados, el dispositivo entonces se desbloquearía únicamente cuando se detecte la yuxtaposición de las características de autenticación referentes al anillo de boda, las palabras, y el fondo. De este modo, puede concederse acceso al usuario al sistema operativo o a características del dispositivo (es decir, contenido del dispositivo).

Debe ponerse de manifiesto para aquellos versados en la materia que son posibles muchas más modificaciones además de aquellas ya descritas, sin desviarse con respecto a los conceptos de la invención en el presente documento. Por lo tanto, la materia objeto de la invención no debe quedar restringida, excepto en el alcance de las reivindicaciones adjuntas. Por otra parte, en la interpretación tanto de la memoria descriptiva como de las reivindicaciones, todos los términos deben interpretarse de la manera más amplia posible congruente con el contexto. En particular, los términos “comprende” y “comprendiendo” deben interpretarse en referencia a los elementos, componentes, o etapas de una manera no excluyente, que indica que los elementos, componentes o etapas a los que se hace referencia pueden estar presentes, o se pueden utilizar, o combinar con otros elementos, componentes, o etapas a los que no se ha hecho referencia expresamente. Cuando las reivindicaciones de la memoria descriptiva se refieren a por lo menos uno de algo seleccionado del grupo consistente en A, B, C ... y N, el texto debe interpretarse de manera que se requiere solamente un elemento del grupo, no A más N, o B más N, etcétera.

REIVINDICACIONES

1. Método de activación de contenido (193, 593) de realidad aumentada, AR, comprendiendo el método:

permitir (610) que un dispositivo electrónico (110, 210) acceda a un agente (180, 580) de autenticación;

obtener (620), por parte del dispositivo electrónico (110, 210), una representación digital (141, 241, 341) de una interacción con un entorno físico (100, 200) que comprende una pluralidad de objetos (120A, 120B, 220, 230, 349A, 349B, 349C);

discriminar (630) por lo menos dos objetos diferentes de entre la pluralidad de objetos (120A, 120B, 220, 230, 349A, 349B, 349C) como primer objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido y segundo objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido, basándose en la representación digital (141, 241, 341);

obtener (640) un primer conjunto de características (160, 260, 360, 460) de autenticación asociadas al primer objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido y un segundo conjunto de características (160, 260, 360, 460) de autenticación asociadas al segundo objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido a partir de la representación digital (141, 241, 341);

caracterizado por que el método comprende además:

establecer (660), por parte del agente (180, 580) de autenticación, un nivel (183, 583) de acceso a contenido, en relación con el contenido de AR, en función de una yuxtaposición (470, 570) del primer conjunto de características (160, 260, 360, 460) de autenticación con respecto al segundo conjunto de características (160, 260, 360, 460) de autenticación, en donde la yuxtaposición (470, 570) se basa en al menos información de tiempo relativo (465);

activar (670), por parte del agente (180, 580) de autenticación, el contenido (193, 593) de AR basándose en el nivel (183, 583) de acceso a contenido y una o más interacciones en el mundo real; y

configurar (680) un dispositivo de salida para presentar el contenido (193, 593) de AR de acuerdo con el nivel (183, 583) de acceso a contenido.

2. Método de la reivindicación 1, en el que por lo menos uno del primer objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido y del segundo objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido comprende un objeto de AR u otro tipo de objeto virtual.

3. Método de la reivindicación 1 ó 2, en el que el contenido (193, 593) de AR comprende un juego, y, en particular,

en donde el nivel (183, 583) de acceso al contenido representa un grado o alcance hasta el cual puede interaccionar un usuario con el juego, y/o

en donde diferentes yuxtaposiciones (470, 570) del primer conjunto de características (160, 260, 360, 460) de autenticación con respecto al segundo conjunto de características (160, 260, 360, 460) de autenticación determinan o permiten diferentes niveles de acceso al juego.

4. Método de cualquiera de las reivindicaciones 1 a 3, en el que la interacción o interacciones en el mundo real incluyen una interacción con una ubicación específica en el mundo real, y/o

en donde la interacción o interacciones en el mundo real incluyen una o más interacciones con otros usuarios del contenido (193, 593) de AR.

5. Método de cualquiera de las reivindicaciones 1 a 4, en el que diferentes yuxtaposiciones (470, 570) del primer conjunto de características (160, 260, 360, 460) de autenticación con respecto al segundo conjunto de características (160, 260, 360, 460) de autenticación permiten diferentes niveles de control sobre el contenido (193, 593) de AR, incluyendo uno o más de autorizar a un usuario a: desplazar en el tiempo el contenido (193, 593) de AR, iniciar o participar en una transacción relacionada con el contenido (193, 593) de AR, copiar o grabar el contenido (193, 593) de AR, editar el contenido (193, 593) de AR, compartir el contenido (193, 593) de AR, e interaccionar de manera directa o indirecta con el contenido (193, 593) de AR.

6. Método de cualquiera de las reivindicaciones 1 a 5, en el que el contenido (193, 593) de AR comprende una promoción asociada a un producto, incluyendo uno o más de un cupón, un mensaje publicitario, una oferta, una rebaja, un número de lotería y un anuncio, y, en particular,

en donde la promoción está asociada a por lo menos uno del primer objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido y el segundo objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido.

7. Método de cualquiera de las reivindicaciones 1 a 6, en el que el contenido (193, 593) de AR comprende por lo menos uno de una aplicación o módulo de software, datos de imagen, datos de vídeo, datos de audio, un historial médico, datos de juego, datos promocionales, información de bienes o servicios, una orden, una instrucción, y una instrucción u orden robótica, y/o

en donde el contenido (193, 593) de AR comprende por lo menos dos modalidades diferentes, incluyendo por lo menos una de una modalidad auditiva, visual, cinestésica, gestual, olfativa, táctil, gustativa, y sensorial, y/o

en donde el contenido (193, 593) de AR comprende por lo menos una de las siguientes: información de transacciones, información de entretenimiento, información de noticias, información deportiva, información promocional, información médica, información de seguridad e información de juegos.

8. Método de cualquiera de las reivindicaciones 1 a 7, que comprende, además, obtener (625) datos multimodales como parte de la representación digital (141, 241, 341), incluyendo por lo menos dos de los siguientes tipos de datos modales: datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración y datos de rumbo, y, en particular,

en donde la obtención (640) de por lo menos uno del primer conjunto de características (160, 260, 360, 460) de autenticación y del segundo conjunto de características (160, 260, 360, 460) de autenticación incluye obtener por lo menos dos conjuntos de características de diferentes modalidades correspondientes a por lo menos dos diferentes de los por lo menos dos tipos de datos modales.

9. Método de cualquiera de las reivindicaciones 1 a 8, en el que la obtención (640) del primer conjunto de características (160, 260, 360, 460) de autenticación incluye obtener características de imagen a partir de datos de imagen del primer objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido en la representación digital, y, en particular,

en donde el primer conjunto de características (160, 260, 360, 460) de autenticación comprende datos de imagen de una parte del primer objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido.

10. Método de cualquiera de las reivindicaciones 1 a 9, en el que la obtención (640) del segundo conjunto de características (160, 260, 360, 460) de autenticación incluye obtener características de imagen a partir de datos de imagen del segundo objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido en la representación digital, y, en particular,

en donde el segundo conjunto de características (160, 260, 360, 460) de autenticación comprende datos de imagen de una parte del segundo objeto (120A, 120B, 220, 230, 349A, 349B, 349C) de autenticación válido.

11. Método de cualquiera de las reivindicaciones 1 a 10, en el que la obtención (640) de por lo menos uno del primer conjunto de características (160, 260, 360, 460) de autenticación y el segundo conjunto de características (160, 260, 360, 460) de autenticación incluye calcular (645) un valor *hash* como característica (160, 260, 360, 460) de autenticación a partir de la representación digital (141, 241, 341), y/o

en donde por lo menos uno del primer conjunto de características (160, 260, 360, 460) de autenticación y del segundo conjunto de características (160, 260, 360, 460) de autenticación incluye por lo menos una de las siguientes: una característica de Transformada de Características Invariantes a la Escala, SIFT, un rasgo de imagen, y una profundidad de campo, y/o

en donde por lo menos uno del primer conjunto de características (160, 260, 360, 460) de autenticación y el segundo conjunto de características (160, 260, 360, 460) de autenticación incluye por lo menos dos de los siguientes tipos de datos de características: datos de imagen, datos de movimiento, datos de audio, datos de temperatura, datos de localización, datos de posición, datos de orientación, metadatos, datos de usuario, datos cinestésicos, datos biométricos, datos de lenguaje, datos de aceleración y datos de rumbo.

12. Método de cualquiera de las reivindicaciones 1 a 11, que comprende, además, activar (670) el contenido (193, 593) de AR en función de criterios desencadenantes de la activación, y, en particular,

en donde los criterios desencadenantes de la activación dependen de un tiempo absoluto, y/o

en donde los criterios desencadenantes de la activación dependen de una o más solicitudes de autenticación.

13. Método de cualquiera de las reivindicaciones 1 a 12, en el que la configuración (680) del dispositivo de salida para que presente el contenido (193, 593) de AR comprende dar instrucciones (681) al dispositivo de salida para que lance una máquina virtual (112).

14. Método de la reivindicación 13, que comprende, además, proteger (683) la máquina virtual (112) con respecto a derechos de contenido de acuerdo con el nivel (183, 583) de acceso a contenido, y/o

que comprende, además, restringir (685) el acceso, por parte de la máquina virtual (112), al contenido (193, 593) de AR de acuerdo con el nivel (183, 583) de acceso a contenido.

15. Método de cualquiera de las reivindicaciones 1 a 14, en el que el dispositivo electrónico (110, 210) comprende por lo menos uno de los siguientes: un teléfono celular, un ordenador de tipo tableta, un ordenador, una consola de juegos, un vehículo, un quiosco interactivo, una máquina expendedora, un robot, un electrodoméstico, un dispositivo médico y un sistema de seguridad, y/o

en donde el dispositivo electrónico (110, 210) comprende el dispositivo de salida.

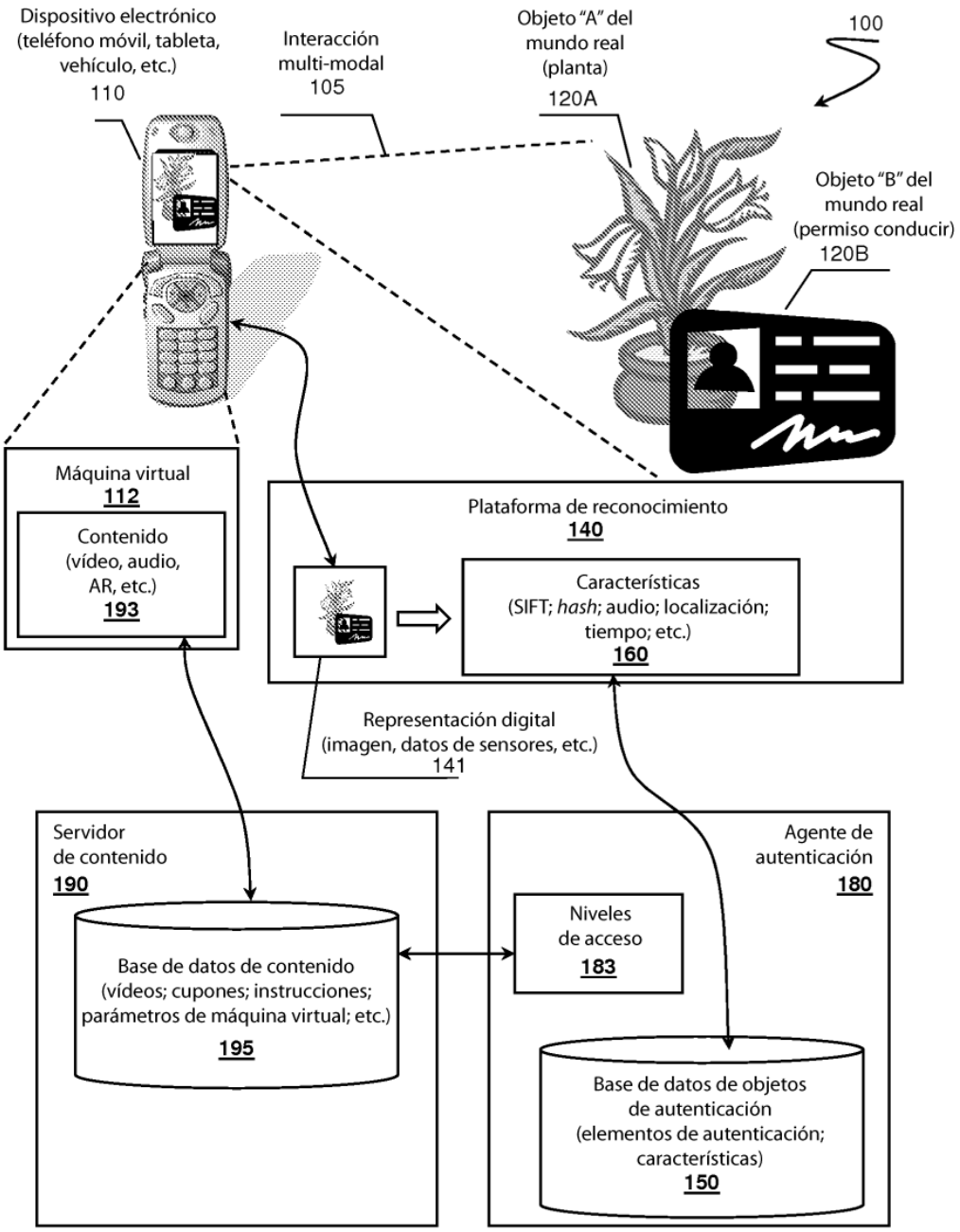
Dispositivo electrónico
(teléfono móvil, tableta,
vehículo, etc.)
110
Interacción
multi-modal
105
Objeto "A" del
mundo real
(planta)
120A
100
Objeto "B" del
mundo real
(permiso conducir)
120B
Máquina virtual
112
Contenido
(vídeo, audio,
AR, etc.)
193
Plataforma de reconocimiento
140
Características
(SIFT; hash; audio; localización;
tiempo; etc.)
160
Representación digital
(imagen, datos de sensores, etc.)
141
Servidor
de contenido
190
Base de datos de contenido
(vídeos; cupones; instrucciones;
parámetros de máquina virtual; etc.)
195
Agente de
autenticación
180
Niveles
de acceso
183
Base de datos de objetos
de autenticación
(elementos de autenticación;
características)
150

Figura 1

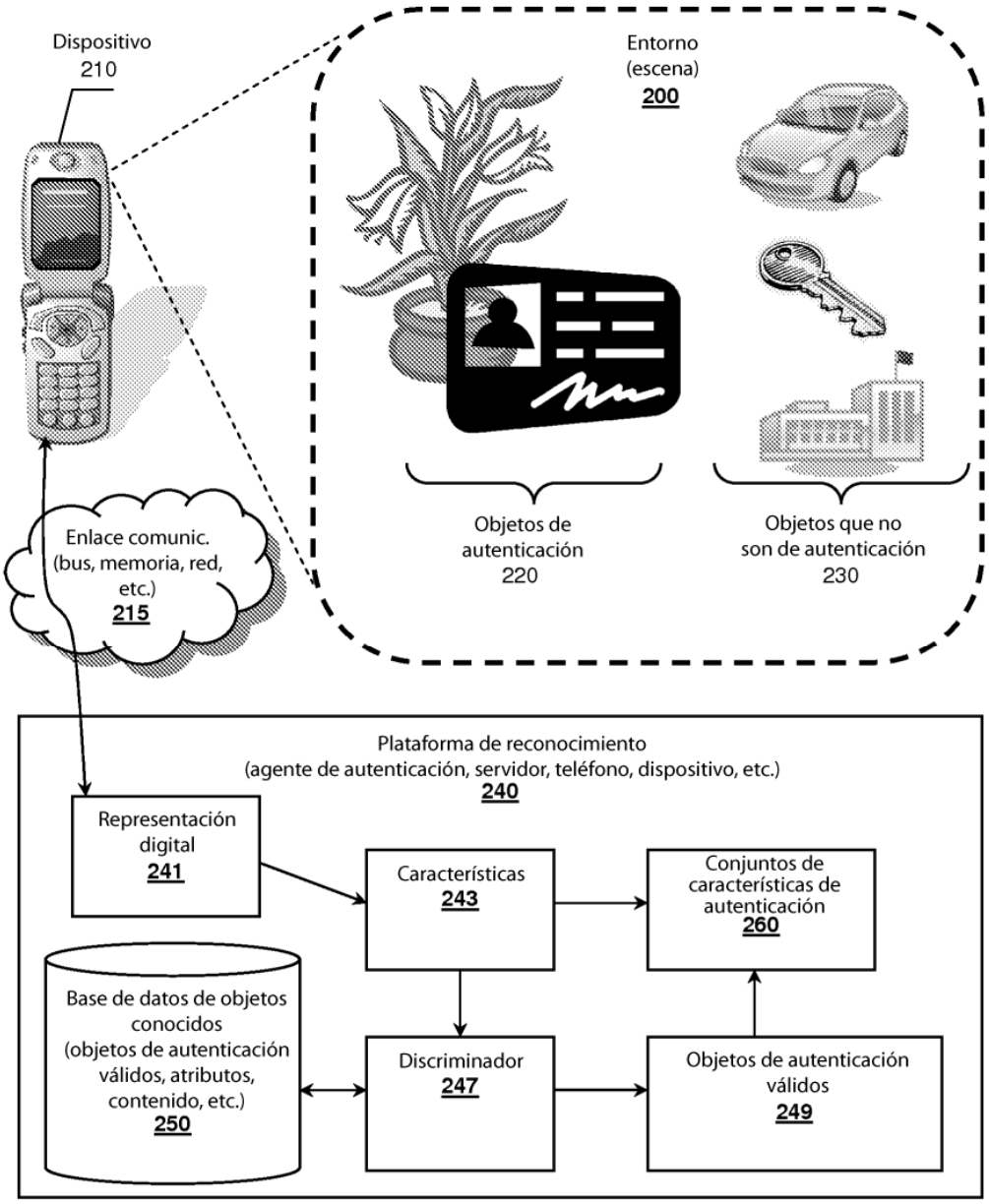
Dispositivo
210
Entorno
(escena)
200
Objetos de
autenticación
220
Objetos que no
son de autenticación
230
Enlace comunic.
(bus, memoria, red,
etc.)
215
Plataforma de reconocimiento
(agente de autenticación, servidor, teléfono, dispositivo, etc.)
240
Representación
digital
241
Características
243
Conjuntos de
características de
autenticación
260
Base de datos de objetos
conocidos
(objetos de autenticación
válidos, atributos,
contenido, etc.)
250
Discriminador
247
Objetos de autenticación
válidos
249

Figura 2

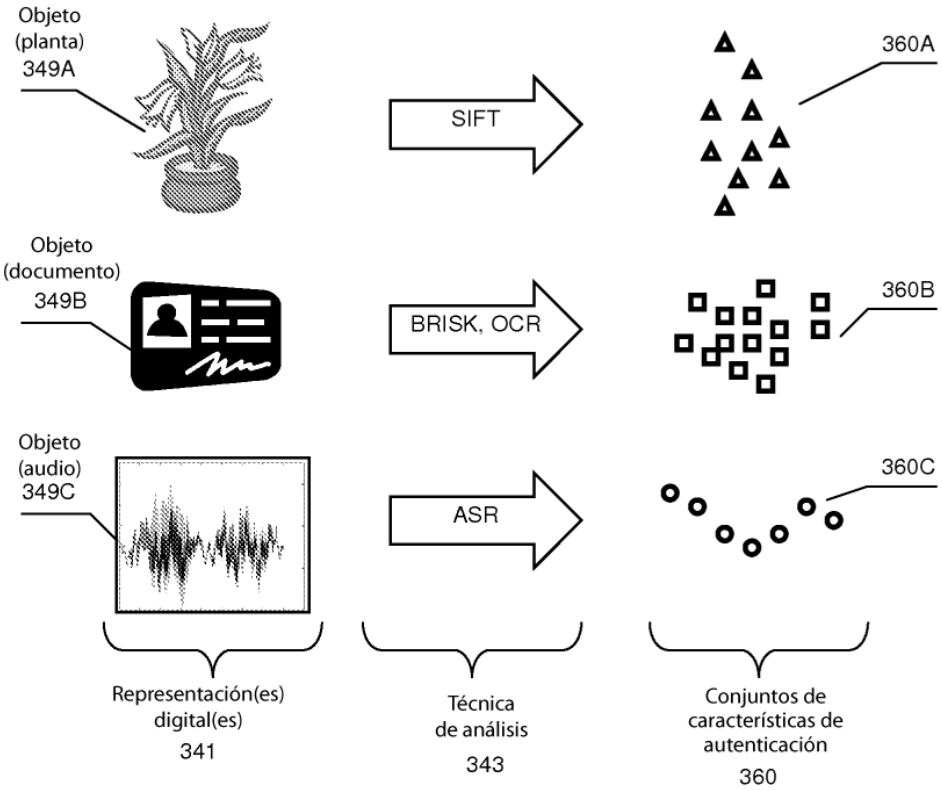
Objeto
(planta)
349A
SIFT
360A
Objeto
(documento)
349B
BRISK, OCR
360B
Objeto
(audio)
349C
ASR
360C
Representación(es)
digital(es)
341
Técnica
de análisis
343
Conjuntos de
características de
autenticación
360

Figura 3

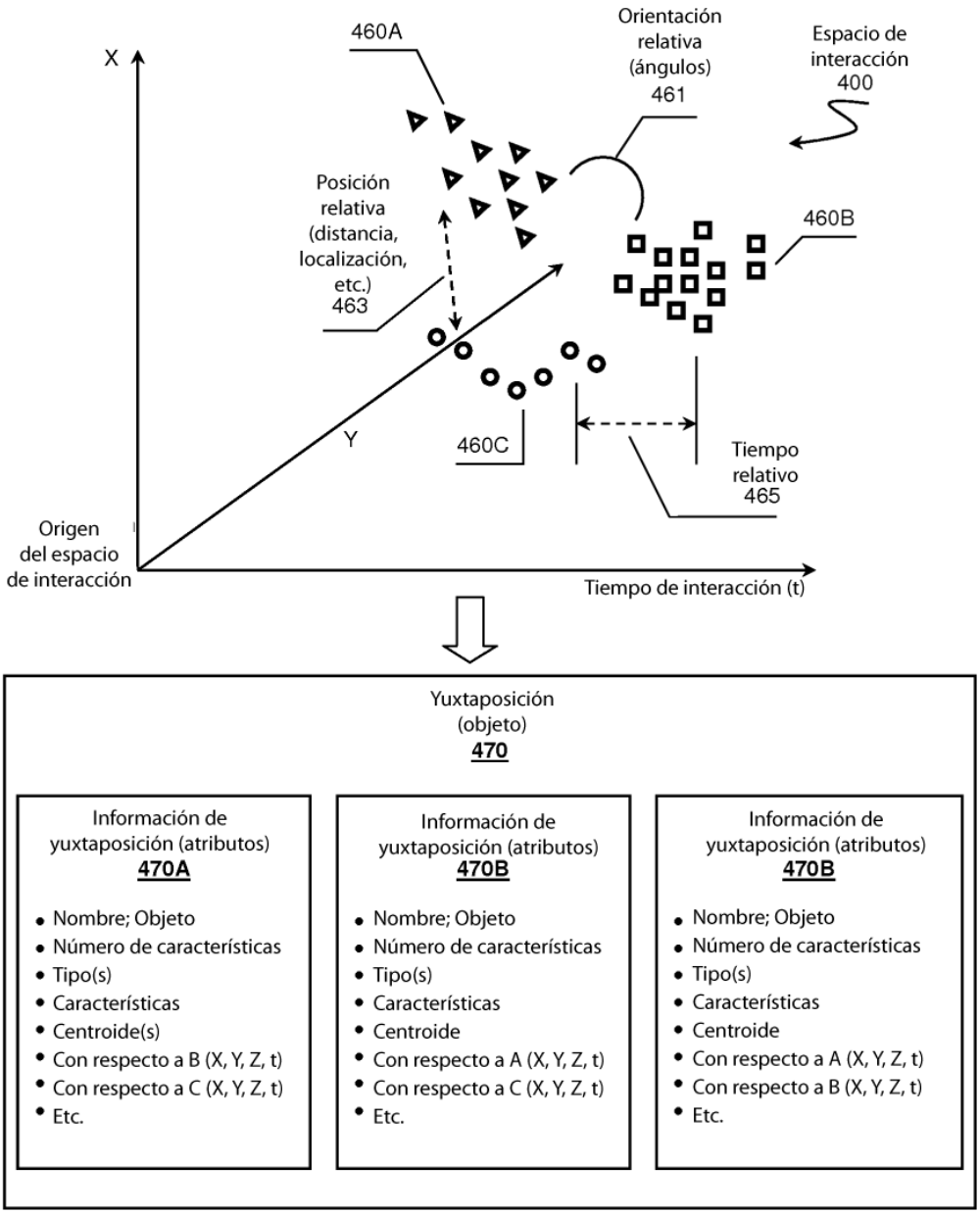
460A
Orientación relativa (ángulos) 461
Espacio de interacción 400
X
Posición relativa (distancia, localización, etc.) 463
460B
Y
460C
Tiempo relativo 465
Origen del espacio de interacción
Tiempo de interacción (t)
Yuxtaposición (objeto) 470
Información de yuxtaposición (atributos) 470A
• Nombre; Objeto
• Número de características
• Tipo(s)
• Características
• Centroide(s)
• Con respecto a B (X, Y, Z, t)
• Con respecto a C (X, Y, Z, t)
• Etc.
Información de yuxtaposición (atributos) 470B
• Nombre; Objeto
• Número de características
• Tipo(s)
• Características
• Centroide
• Con respecto a A (X, Y, Z, t)
• Con respecto a C (X, Y, Z, t)
• Etc.
Información de yuxtaposición (atributos) 470B
• Nombre; Objeto
• Número de características
• Tipo(s)
• Características
• Centroide
• Con respecto a A (X, Y, Z, t)
• Con respecto a B (X, Y, Z, t)
• Etc.

Figura 4

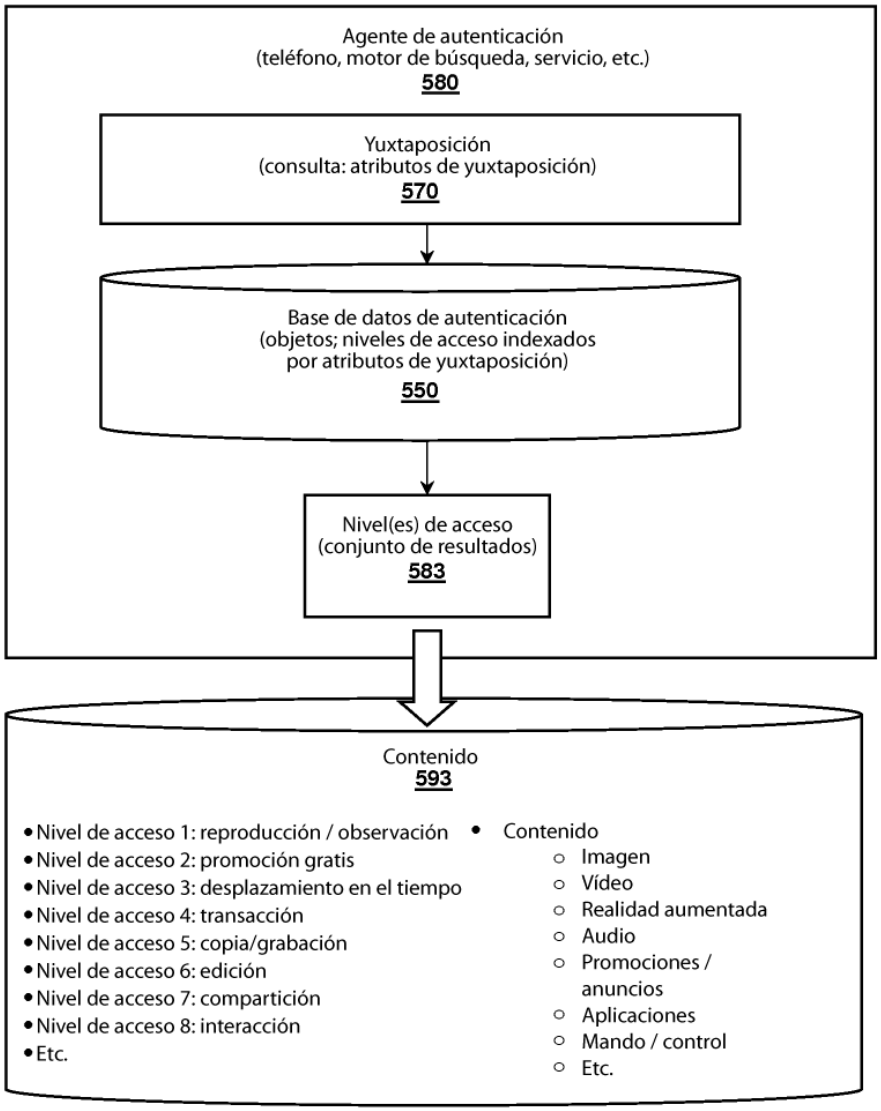
Agente de autenticación
(teléfono, motor de búsqueda, servicio, etc.)
580
Yuxtaposición
(consulta: atributos de yuxtaposición)
570
Base de datos de autenticación
(objetos; niveles de acceso indexados
por atributos de yuxtaposición)
550
Nivel(es) de acceso
(conjunto de resultados)
583
Contenido
593
• Nivel de acceso 1: reproducción / observación
• Nivel de acceso 2: promoción gratis
• Nivel de acceso 3: desplazamiento en el tiempo
• Nivel de acceso 4: transacción
• Nivel de acceso 5: copia/grabación
• Nivel de acceso 6: edición
• Nivel de acceso 7: compartición
• Nivel de acceso 8: interacción
• Etc.
• Contenido
○ Imagen
○ Vídeo
○ Realidad aumentada
○ Audio
○ Promociones / anuncios
○ Aplicaciones
○ Mando / control
○ Etc.

Figura 5

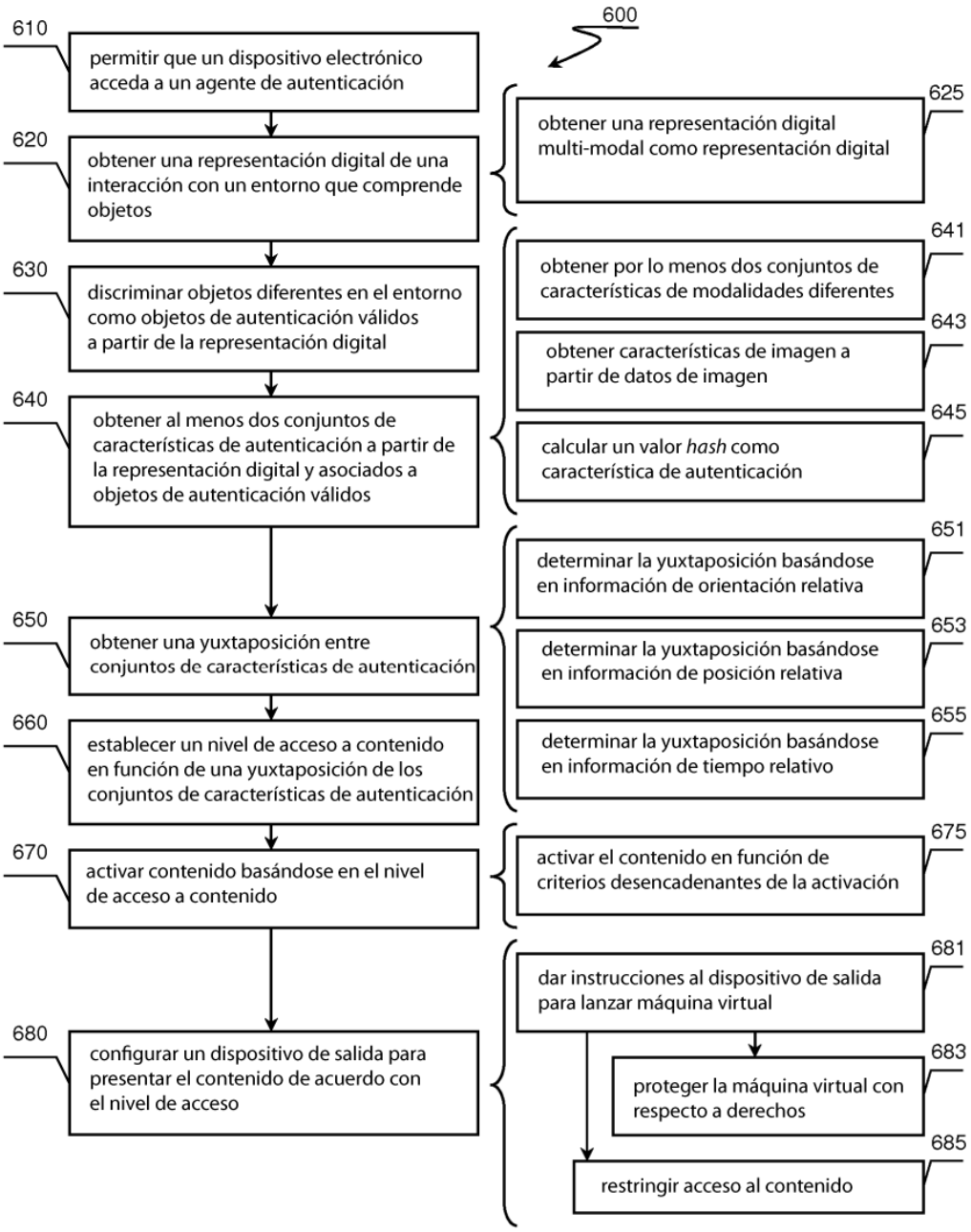
600
610
permitir que un dispositivo electrónico acceda a un agente de autenticación
620
obtener una representación digital de una interacción con un entorno que comprende objetos
625
obtener una representación digital multi-modal como representación digital
630
discriminar objetos diferentes en el entorno como objetos de autenticación válidos a partir de la representación digital
640
obtener al menos dos conjuntos de características de autenticación a partir de la representación digital y asociados a objetos de autenticación válidos
641
obtener por lo menos dos conjuntos de características de modalidades diferentes
643
obtener características de imagen a partir de datos de imagen
645
calcular un valor *hash* como característica de autenticación
650
obtener una yuxtaposición entre conjuntos de características de autenticación
651
determinar la yuxtaposición basándose en información de orientación relativa
653
determinar la yuxtaposición basándose en información de posición relativa
655
determinar la yuxtaposición basándose en información de tiempo relativo
660
establecer un nivel de acceso a contenido en función de una yuxtaposición de los conjuntos de características de autenticación
670
activar contenido basándose en el nivel de acceso a contenido
675
activar el contenido en función de criterios desencadenantes de la activación
680
configurar un dispositivo de salida para presentar el contenido de acuerdo con el nivel de acceso
681
dar instrucciones al dispositivo de salida para lanzar máquina virtual
683
proteger la máquina virtual con respecto a derechos
685
restringir acceso al contenido

Figura 6