(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 762 524**

(51) Int. CI.:

H04M 1/00 (2006.01)
H04W 12/06 (2009.01)
G06F 21/32 (2013.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
G06K 9/00 (2006.01)
H04L 29/06 (2006.01)
G07F 19/00 (2006.01)
G06K 9/46 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.05.2014 PCT/US2014/037871**

(87) Fecha y número de publicación internacional: **20.11.2014 WO14186374**

(96) Fecha de presentación y número de la solicitud europea: **13.05.2014 E 14797820 (9)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2997719**

(54) Título: **Sistema y método para autorizar el acceso a entornos de acceso controlado**

(30) Prioridad:

13.05.2013 US 201361822746 P
03.07.2013 US 201361842800 P
03.07.2013 US 201361842757 P
03.07.2013 US 201361842739 P
03.07.2013 US 201361842756 P
26.12.2013 US 201361921004 P
26.12.2013 US 201361920985 P
31.12.2013 US 201361922438 P
06.01.2014 US 201461924092 P
06.01.2014 US 201461924097 P
07.03.2014 US 201414201499
07.03.2014 US 201414201462
07.03.2014 US 201414201438

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.05.2020

(73) Titular/es:

VERIDIUM IP LIMITED (100.0%)
100 New Bridge Street
London EC4V 6JA, GB

(72) Inventor/es:

HOYOS, HECTOR;
BRAVERMAN, JASON;
XIAO, GEOFFREY;
STREIT, SCOTT y
MATHER, JONATHAN FRANCIS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método para autorizar el acceso a entornos de acceso controlado

Referencia a aplicaciones relacionadas

La presente solicitud hace referencia a la Solicitud de Patente de los Estados Unidos de Nº de serie 61/822.746, titulada “SYSTEM AND METHOD FOR PROVIDING BIOMETRICALLY AUTHENTICATED ACCESS USING MOBILE DEVICES”, presentada el 13 de mayo de 2013; la Solicitud de Patente de los Estados Unidos de Nº de serie 61/842.800, titulada “SYSTEM AND METHOD FOR PROVIDING BIOMETRICALLY AUTHENTICATED ACCESS USING MOBILE DEVICES”, presentada el 3 de julio de 2013; la Solicitud de Patente de los Estados Unidos, de Nº de serie 61/842.739, titulada “SECURE BACK-END ARCHITECTURE SYSTEM AND METHOD”, presentada el 3 de julio de 2013; la Solicitud de Patente de los Estados Unidos de Nº de serie 61/842.757, titulada “SYSTEM AND METHOD FOR GENERATING A BIOMETRIC IDENTIFIER”, presentada el 3 de julio de 2013; la Solicitud de Patente de los Estados Unidos de Nº de serie 61/842.756, titulada “SYSTEMS AND METHODS FOR DETERMINING LIVENESS”, presentada el 3 de julio de 2013; la Solicitud de Patente Provisional de los Estados Unidos de Nº de serie 61/921.004, titulada “SYSTEM AND METHOD FOR DETERMINING LIVENESS», presentada el 26 de diciembre de 2013; la Solicitud de Patente Provisional de los Estados Unidos de Nº de serie 61/920.985, titulada “SYSTEM AND METHOD FOR GENERATING A BIOMETRIC IDENTIFIER”, presentada el 26 de diciembre de 2013; la Solicitud de Patente Provisional de los Estados Unidos de Nº de serie 61/922.438, titulada “SYSTEM AND METHOD FOR BIOMETRIC PROTOCOL STANDARDS”, presentada el 31 de diciembre de 2013; la Solicitud de Patente de los Estados Unidos de Nº de serie 61/924.092, titulada “SECURE BACK-END ARCHITECTURE SYSTEM AND METHOD”, presentada el 6 de enero de 2014; la Solicitud de Patente de los Estados Unidos de Nº de serie 61/924.097, titulada “SYSTEM AND METHOD FOR SMARTPHONE SECURITY CASE”, presentada el 6 de enero de 2014; la Solicitud de Patente de los Estados Unidos de Nº de serie 14/201.438, titulada “SYSTEMS AND METHODS FOR BIOMETRIC AUTHENTICATION OF TRANSACTIONS”, presentada el 7 de marzo de 2014; la Solicitud de Patente de los Estados Unidos de Nº de serie 14/201.462, titulada “SYSTEMS AND METHODS FOR DETERMINING LIVENESS”, presentada el 7 de marzo de 2014; y la Solicitud de Patente de los Estados Unidos de Nº de serie 14/201.499, titulada “SYSTEM AND METHOD FOR GENERATING A BIOMETRIC IDENTIFIER”, presentada el 7 de marzo de 2014.

Campo técnico de la invención

La presente invención hace referencia a sistemas y métodos para proporcionar un acceso autenticado, en particular, a sistemas y métodos para proporcionar un acceso autenticado de manera biométrica utilizando un dispositivo móvil.

Antecedentes de la invención

Existen sistemas de acceso seguro para realizar la autenticación de dos factores para un usuario a un recurso de red (por ejemplo, servidores remotos, puntos de acceso bloqueados de manera electrónica, etc.). Un ejemplo de sistema de autenticación de dos factores es el mecanismo de autenticación RSA SecurID®, comercializado por la firma EMC Corporation, de Bedford Mass. Este sistema a modo de ejemplo consiste en un “token”, ya sea hardware (por ejemplo, un pincho USB) o software (un token de software), que se asigna para un usuario de ordenador y que genera un código de autenticación a intervalos fijos (generalmente 60 segundos) utilizando un reloj incorporado y la clave aleatoria, codificada en fábrica, de la tarjeta (conocida como “registro de semilla”). El registro de semilla es diferente para cada token y es cargado en el servidor del sistema correspondiente a medida que se compran los tokens. El usuario que se autentica debe introducir un número de identificación personal (PIN - Personal Identification Number, en inglés) y el código de autenticación generado que se muestra en ese momento.

No obstante, las mayores infracciones se han producido en dichos sistemas, tales como el fallo de seguridad de RSA en 2011, que culminó con la filtración de datos confidenciales de grandes corporaciones hacia fuentes desconocidas. Conocer los registros de semilla permite a un atacante un acceso completo a la información de un usuario, y acceso a cualquier cosa que pueda utilizar con sus claves.

Pretty Good Privacy (PGP) es un programa informático de cifrado y descifrado de datos que proporciona privacidad criptográfica y autenticación para la comunicación de datos. El PGP se puede utilizar para firmar, cifrar y descifrar textos, correos electrónicos, archivos, directorios y particiones de disco completo para aumentar la seguridad de las comunicaciones mediante correo electrónico. El PGP y otros métodos de cifrado de clave privada son muy seguros, siempre y cuando ciertas circunstancias sigan siendo ciertas. En cualquier intercambio de clave privada, si la clave privada se pierde, es robada o se extravía, los datos del usuario están completamente abiertos. Por el contrario, si el usuario pierde la clave, los datos que está protegiendo se pierden para siempre. Por lo tanto, el problema es evidente.

Se han propuesto numerosas técnicas en la literatura para tratar el problema del robo de identidad. Cualquier esquema de este tipo intenta establecer que una persona es quien dice ser. Las contraseñas, las claves privadas (largas) y el camuflaje son algunos de los enfoques utilizados para este propósito. Puesto que los seres humanos no pueden recordar las claves largas, las claves privadas a menudo tienden a ser almacenadas en una billetera cifrada posiblemente mediante una contraseña pequeña. Desgraciadamente, todos estos esquemas tienen la propiedad de

que alguien que tenga estas credenciales (tales como las claves y contraseñas correctas) será aceptado como la persona correcta, incluso si estas credenciales han sido robadas de otros.

Puesto que un dato biométrico es una característica biológica (tal como una huella digital, la geometría de una mano, el patrón de retina, la forma del iris, etc.) de un individuo, las técnicas biométricas se pueden utilizar como un factor de verificación adicional, ya que los datos biométricos suelen ser más difíciles de obtener que otras credenciales no biométricas. Los datos biométricos se pueden utilizar para la identificación y/o autenticación (también denominada afirmación y/o verificación de identidad).

La afirmación de identidad biométrica puede requerir un cierto nivel de seguridad según lo dicte la aplicación. Por ejemplo, la autenticación en relación con una transacción financiera, o la obtención de acceso a una ubicación segura requiere niveles de seguridad más altos. Como resultado, preferiblemente, la precisión de la representación biométrica de un usuario es suficiente para garantizar que el usuario se autentique con precisión y se mantenga la seguridad. No obstante, en la medida en que existan sistemas de afirmación de identidad de iris, cara, dedos y voz y proporcionen el nivel de precisión requerido, dichos sistemas requieren dispositivos y aplicaciones exclusivos, y no son implementados fácilmente en teléfonos inteligentes convencionales, que tienen una resolución limitada de la cámara y capacidades de emisión de luz.

Los problemas que rodean a las técnicas tradicionales de captura de características biométricas, que, en general, requieren imágenes de alta resolución, iluminación multiespectral y una potencia informática importante, para ejecutar los algoritmos de análisis de imágenes existentes con el fin de lograr la precisión requerida dictada por la seguridad, han hecho que la autenticación biométrica no esté disponible de manera extendida o sea accesible para las masas. Además, las técnicas tradicionales de autenticación biométrica que requieren dispositivos exclusivos utilizados de una manera específica (por ejemplo, requieren un asunto colaborativo, tienen un campo de visión reducido, el dato biométrico debe ser obtenido de una manera específica) van en contra de la comodidad del usuario y de la implementación a gran escala.

En consecuencia, existe la necesidad de sistemas y métodos con los que se pueda verificar de manera cómoda la identidad de un usuario, sin interrupciones y con un grado suficiente de precisión, a partir de la información biométrica capturada por el usuario utilizando teléfonos inteligentes fácilmente disponibles. Además, lo que se necesita son sistemas y métodos de afirmación de identidad que, preferiblemente, no dependan de dispositivos de imágenes multiespectrales, emisores de luz multiespectrales, cámaras de alta resolución o múltiples entradas de usuario.

El documento WO2007/019351 da a conocer un dispositivo de identificación y autenticación de usuario que proporciona una plataforma informática segura y una ruta informática segura para la comunicación con un ordenador principal remoto seguro. El dispositivo está conectado a un PC inseguro, pero proporciona una verificación segura de la identidad de un usuario y la autorización para participar en una transacción.

El documento WO2012/123727 da a conocer un sistema de comunicación de datos en el que un proveedor de autorización proporciona la autorización de un abonado a un servicio de autorización. El sistema de comunicaciones de datos incluye una pluralidad de partes que confían y una pluralidad de proveedores de autorización. Se recibe una solicitud de autorización que incluye datos que identifican a un abonado de un servicio de autorización de una parte que confía. Un proveedor de autorización se selecciona de la pluralidad de proveedores de autorización sobre la base de los datos de identificación del abonado. Una solicitud de autorización es transmitida al proveedor de autorización seleccionado. Una respuesta de autorización es recibida del proveedor de autorización seleccionado. La respuesta de autorización indica que el abonado ha autorizado la solicitud en un dispositivo de telecomunicaciones con el que el proveedor de autorización ha iniciado el contacto, en respuesta a la solicitud de autorización. Se transmite un mensaje de autorización a la parte que confía en base, al menos en parte, a la respuesta de autorización recibida del proveedor de autorización seleccionado.

Compendio de la invención

Las tecnologías se presentan en el presente documento para soportar un sistema y un método para autorizar el acceso de un usuario a un entorno de acceso controlado.

Según un primer aspecto, la presente invención da a conocer un método para autorizar a un usuario a acceder a un entorno de acceso controlado, tal como se define en la reivindicación 1.

Según otro aspecto, la presente invención da a conocer un sistema para autorizar el acceso a un entorno de acceso controlado, tal como se define en la reivindicación 12.

Estos y otros aspectos, características y ventajas se pueden apreciar a partir de la descripción adjunta de ciertas realizaciones de la invención, y de las figuras y reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 es un diagrama de alto nivel de un sistema para autorizar el acceso a un entorno de acceso controlado, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 2A es un diagrama de bloques de un dispositivo informático, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 2B es un diagrama de bloques de módulos de software informático, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 2C es un diagrama de bloques de un dispositivo informático, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 3 es un diagrama de flujo que muestra una rutina para inscribir a un usuario de acuerdo con las características biométricas del usuario, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 4 es un diagrama de flujo que muestra una rutina para autorizar el acceso a un entorno de acceso controlado, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 5 es un diagrama de flujo que muestra una rutina para autenticar a un usuario de acuerdo con las características biométricas del usuario, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 6A es una captura de pantalla de una interfaz de usuario, a modo de ejemplo, de acuerdo con al menos una realización dada a conocer en el presente documento;

la figura 6B es una captura de pantalla de una interfaz de usuario, a modo de ejemplo, de acuerdo con al menos una realización dada a conocer en el presente documento; y

la figura 7 es un diagrama de flujo que muestra una rutina para determinar la vitalidad, de acuerdo con al menos una realización dada a conocer en el presente documento.

Descripción detallada de ciertas realizaciones de la invención

Solo a modo de ejemplo, y con el propósito de visión general e introducción, a continuación, se describen realizaciones de la presente invención que hacen referencia a un sistema y un método para autorizar el acceso de un usuario a un entorno de acceso controlado (ACE - Access Controlled Environment, en inglés), de acuerdo con las características biométricas del usuario.

En algunas implementaciones, el sistema incluye una plataforma de servidor de un sistema basado en la nube que se comunica con un PC, con servidores y con dispositivos fijos, tales como ordenadores portátiles, tabletas y teléfonos inteligentes operados por usuarios. A medida que el usuario intenta acceder a un entorno de red de acceso controlado, por ejemplo, a un sitio web que requiere un inicio de sesión seguro, se le solicita que se autentique utilizando el dispositivo móvil, registrado previamente, del usuario. La autenticación incluye capturar información biométrica en la forma de, al menos, imágenes de los ojos, región periocular y cara del usuario, o cualquier combinación de lo anterior (en conjunto, la región de Vitruvio), extraer características únicas y codificar las características como un identificador (“Identificador de Vitruvio”) utilizando el dispositivo móvil. El sistema puede generar, asimismo, un identificador único de dispositivo móvil, de acuerdo con la información de identificación única asociada con el dispositivo móvil. El usuario puede ser autenticado de acuerdo con la información biométrica y con la información del dispositivo móvil, ya sea mediante el dispositivo móvil o mediante el servidor del sistema, o una combinación de ambos. La autenticación del usuario puede incluir, asimismo, determinar si la información biométrica y otra información no biométrica indica que el usuario es un sujeto vivo, y no una reproducción de imagen o video que intenta suplantar la identidad para el sistema. Si el usuario se autentica correctamente, el sistema puede conceder acceso de manera electrónica al entorno de red al que el usuario intenta acceder. Por ejemplo, mediante la transmisión de una notificación de autorización a un dispositivo informático de un tercero. De esta manera a modo de ejemplo, el sistema de autenticación segura puede ser utilizado para autenticar el acceso del usuario a sitios web, VPN, acceso en una puerta física, acceso en un cajero automático, transacciones financieras o acceso a cualquier sistema informático que requiera identificación / autenticación del usuario.

Los sistemas y métodos de la presente solicitud proporcionan una gran comodidad para los usuarios en función de la gestión del acceso basado en datos biométricos, y una mayor seguridad de las transacciones, complementando o eliminando la necesidad de contraseñas y/o dispositivos exclusivos para el almacenamiento de información de la cuenta del usuario, tales como tarjetas o claves de token y similares. Se establece que muchos de los principios dados a conocer en el presente documento son aplicables a prácticamente cualquier tipo de sistema que requiera autenticación de usuario, tal como, por ejemplo, acceso a sitios web, control de acceso físico, inicio, determinación de funciones de usuario, identificación de grupo, automatización, gestión de contraseñas u otro acceso. La presente

solicitud elimina la necesidad de contraseñas, pines, tokens o similares, de cualquier entorno informático, incluidas las redes informáticas mundiales.

Según un aspecto destacado de la solicitud en cuestión, la captura de imágenes con el fin de identificar las características biométricas de Vitruvio de un usuario se puede realizar utilizando cámaras digitales convencionales que se encuentran comúnmente en teléfonos inteligentes y en otros dispositivos móviles. Además, la identificación de las características biométricas de Vitruvio se puede realizar de acuerdo con técnicas positivas de autenticación ocular, preferiblemente, aplicando algoritmos que analizan el iris y/o las regiones perioculares y/o la cara, sin requerir imágenes infrarrojas o emisores de IR que no están ampliamente integrados en los teléfonos inteligentes.

De acuerdo con un aspecto destacado de la aplicación en cuestión, las características biométricas del iris del usuario, las regiones perioculares y/o faciales se pueden extraer, de manera simultánea y sin problemas, de las capturas de imágenes comunes (por ejemplo, los mismos fotogramas de imagen y la misma secuencia de fotogramas de imagen capturados), mientras que las técnicas de identificación actuales, en general, extraen las características del iris de ciertos fotogramas de imagen y las características perioculares de otros fotogramas de imagen. Además, de acuerdo con otro aspecto destacado de la solicitud del asunto, las características biométricas de Vitruvio se identifican y definen de acuerdo con la relación espacial de las características ("puntos clave") dentro de un solo fotograma y con el movimiento dinámico o posición ("flujo") de esos puntos clave a lo largo de una secuencia de fotogramas organizada temporalmente, para generar a la perfección un identificador biométrico de Vitruvio integrado de la región de Vitruvio del usuario. El identificador biométrico de Vitruvio integrado resultante es una representación virtual única de la región de Vitruvio del usuario, en lugar de generar, de manera independiente, una pluralidad de identificadores biométricos separados (por ejemplo, uno para el iris, otro para la región periocular) que son fusionados posteriormente. Se puede apreciar que los identificadores pueden ser codificados como uno o más vectores, incluida la información biométrica y no biométrica.

La presente invención describe, asimismo, técnicas adicionales para impedir la autenticación errónea causada por una suplantación de identidad. En algunos ejemplos, las técnicas anti-suplantación de identidad pueden incluir capturar múltiples imágenes faciales de un usuario y analizar las imágenes faciales en busca de indicios de vitalidad. Un aspecto destacado de la solicitud del asunto es que el proceso para generar un identificador de Vitruvio que incluye información relacionada con el movimiento dinámico de puntos clave es representativo de vitalidad, y/o se puede utilizar, asimismo, para generar un identificador de vitalidad. Utilizando el identificador de vitalidad, el sistema dado a conocer puede determinar la "vitalidad" (por ejemplo, si la secuencia de imágenes es de un usuario vivo) y detectar intentos sospechosos de suplantación de identidad, mediante la comparación del identificador de vitalidad actual con un identificador de vitalidad generado previamente. Además, la vitalidad puede ser determinada a partir del análisis del movimiento dinámico de las características de Vitruvio de bajo nivel para determinar si el flujo es representativo de un movimiento continuo. La vitalidad también puede ser indicada por el movimiento de características de nivel intermedio, tales como los ojos, la boca y otras partes de la cara. Dichos programas anti-suplantación de identidad pueden, en diversas implementaciones, detectar movimientos faciales en base a áreas específicas del rostro humano. Por ejemplo, los programas anti-suplantación de identidad pueden identificar uno o los dos ojos de la imagen facial como puntos de referencia. Los programas anti-suplantación de identidad pueden detectar y analizar las transiciones entre las imágenes en relación con uno o con los dos ojos. Utilizando cualquier transición detectada, los programas anti-suplantación de identidad pueden detectar gestos faciales tales como un parpadeo y similares. En base al análisis y a la detección de un resultado satisfactorio, los programas de determinación de la vitalidad pueden impedir o conceder acceso a funcionalidades controladas por el dispositivo informático.

Un sistema a modo de ejemplo para autorizar el acceso a un entorno de acceso controlado 100 se muestra como un diagrama de bloques en la figura 1. En una disposición, el sistema consiste en un servidor de sistema 105 y en uno o más dispositivos de usuario 101 que incluyen un dispositivo móvil 101a y un dispositivo informático 101b. El sistema 100 puede incluir, asimismo, uno o más dispositivos informáticos remotos 102.

El servidor 105 del sistema puede ser prácticamente cualquier dispositivo informático y/o aparato de procesamiento de datos capaz de comunicarse con los dispositivos de usuario y con dispositivos informáticos remotos y recibir, transmitir y almacenar información electrónica, y procesar solicitudes, tal como se describe adicionalmente en el presente documento. De manera similar, el dispositivo informático remoto 102 puede ser prácticamente cualquier dispositivo informático y/o aparato de procesamiento de datos capaz de comunicarse con el servidor del sistema y/o con los dispositivos de usuario y recibir, transmitir y almacenar información electrónica, y procesar solicitudes, tal como se describe adicionalmente en el presente documento. Se debe comprender, asimismo, que el servidor del sistema y/o el dispositivo informático remoto pueden ser varios dispositivos informáticos en red o basados en la nube.

En algunas implementaciones, el dispositivo informático 102 puede estar asociado con una organización de una empresa que mantiene cuentas de usuario y requiere la autenticación de los titulares de cuentas antes de conceder acceso a entornos de red seguros (por ejemplo, un sitio web seguro, un banco, una VPN, proveedores de pago y similares). Los diversos tipos de cuentas de usuario utilizadas para acceder o interactuar con dichos entornos en red se denominan, en el presente documento, cuentas de transacción.

Los dispositivos de usuario, el dispositivo móvil 101a y el dispositivo informático 101b del usuario pueden estar configurados para comunicarse entre sí, con el servidor 105 del sistema y/o con un dispositivo informático remoto 102, transmitiendo información electrónica al mismo y recibiendo información electrónica del mismo, tal como se describe adicionalmente en el presente documento. Los dispositivos de usuario pueden ser configurados, asimismo, para recibir entradas de usuario, así como capturar y procesar información biométrica, por ejemplo, imágenes digitales y grabaciones de voz de un usuario 124.

El dispositivo móvil 101a puede ser cualquier dispositivo informático móvil y/o aparato de procesamiento de datos capaz de tener incorporados los sistemas y/o métodos descritos en el presente documento, incluyendo, entre otros, un ordenador personal, una tableta, un asistente digital personal, un dispositivo electrónico móvil, un teléfono celular o un dispositivo de teléfono inteligente, y similares. El dispositivo informático 101b está destinado a representar diversas formas de dispositivos informáticos con los que un usuario puede interactuar, tales como puestos de trabajo, un ordenador personal, un ordenador portátil, sistemas dedicados de punto de venta, terminales de cajero automático, dispositivos de control de acceso u otros ordenadores digitales apropiados.

Tal como se describe adicionalmente en el presente documento, el sistema para autorizar el acceso a un entorno de acceso controlado 100, facilita la autenticación de un usuario 124 de acuerdo con las características biométricas de un usuario utilizando un dispositivo móvil 101a. En algunas implementaciones, la identificación y/o autenticación de acuerdo con las características biométricas de un usuario utiliza la información biométrica de un usuario en un proceso de dos etapas. La primera etapa se conoce como inscripción. En la etapa de inscripción, se recogen muestras (por ejemplo, imágenes) de datos biométricos apropiados de un individuo. Estas muestras de datos biométricos son analizadas y procesadas para extraer las funcionalidades (o características) presentes en cada muestra. El conjunto de características presentes en los datos biométricos de un individuo constituye un identificador para la persona e indica si el usuario es un sujeto vivo. Estos identificadores son almacenados para completar la etapa de inscripción. En la segunda etapa se mide el mismo dato biométrico del individuo. Las características de estos datos biométricos se extraen al igual que en la fase de inscripción para obtener un identificador biométrico actual. Si el objetivo es determinar la vitalidad, las funcionalidades o características se pueden analizar para determinar si son representativas de un sujeto vivo. Si el objetivo es la identificación, este identificador es buscado en la base de datos de identificadores generados en la primera fase. Si se produce una coincidencia, la identificación del individuo es revelada; en caso contrario, la identificación falla. Si el objetivo es la autenticación, el identificador generado en la segunda etapa es comparado con el identificador generado en la primera etapa para la persona concreta. Si se produce una coincidencia, la autenticación se realiza correctamente; de lo contrario, la autenticación falla.

En algunas implementaciones, el servidor del sistema puede ser configurado para facilitar de manera segura la identificación / autenticación de la identidad del usuario (denominada conjuntamente “afirmación de identidad”) en el desarrollo de una transacción, sin autorizar la transacción subyacente. De esta manera, no es necesario que el servidor guarde la información confidencial de la cuenta de la transacción del usuario que se utiliza para autorizar la transacción subyacente; por el contrario, el servidor del sistema está configurado para autorizar a un usuario mediante el reconocimiento de un usuario en lugar de otro con un nivel de seguridad apropiado. Por ejemplo, afirmar la identidad de un usuario que realiza una transacción bancaria de acuerdo con los estándares requeridos por el banco y notificar al sistema informático corporativo del banco (por ejemplo, el dispositivo informático remoto 102) que el usuario ha sido autenticado. En consecuencia, los sistemas y métodos a modo de ejemplo pueden complementar y/o reemplazar los procesos de autenticación corporativa existentes mediante la integración con la infraestructura y los procesos existentes sin interferir con los procesos establecidos para autorizar las transacciones una vez que se ha establecido la identidad de un usuario, por motivos de seguridad.

Además de la afirmación de identidad, el servidor 105 del sistema puede implementar, asimismo, procesos de seguridad adicionales, que incluyen la recopilación de funciones y el control de acceso, para facilitar la autorización de transacciones electrónicas solicitadas o controlar de otro modo el acceso de un usuario. De este modo, el proceso de autorización del usuario puede incluir la afirmación de identidad, y puede incluir, asimismo, la autorización, mediante la determinación de si la identidad del usuario está asociada con una o más cuentas de transacción. Además, el proceso de autorización de la transacción puede incluir, asimismo, la determinación del nivel de acceso del usuario utilizando la cuenta de la transacción, por ejemplo, si el usuario tiene los permisos necesarios para realizar las transacciones solicitadas en un cajero automático.

En algunas implementaciones, el servidor 105 del sistema puede implementar, asimismo, reglas que rigen el acceso a la información y/o la transmisión de información entre una variedad de dispositivos informáticos con los que los usuarios pueden interactuar (por ejemplo, un dispositivo móvil 101a, un dispositivo informático 101b) y uno o más de servidores de confianza del lado del servidor (por ejemplo, el servidor 105 del sistema y el dispositivo informático remoto 102). De manera más específica, el servidor 105 del sistema puede hacer cumplir las reglas que rigen el acceso del usuario a la información, así como el intercambio de información con terceros según lo autorice el usuario. Por ejemplo, el servidor del sistema puede regular el acceso a una base de datos de información perteneciente a un usuario y que ha sido autenticada de manera biométrica por el usuario, y limitar el acceso a esa información de acuerdo con reglas definidas por el usuario. A modo de ejemplo adicional, mantener una base de datos de información y conceder acceso a la información a un usuario autenticado de acuerdo con reglas o permisos previamente concedidos al usuario.

Los sistemas y métodos a modo de ejemplo para facilitar la afirmación de la identidad, la recopilación de funciones, el control de acceso y otras funciones de seguridad del servidor 105 del sistema, incluida la auditoría y la garantía de la seguridad y las responsabilidades, se describen más detalladamente en el presente documento y en la Solicitud de Patente Provisional de los Estados Unidos de Nº de serie 61/922.438, titulada “SYSTEM AND METHOD FOR BIOMETRIC PROTOCOL STANDARDS”, presentada el 31 de diciembre de 2013, en tramitación con la presente y comúnmente asignada.

Cabe señalar que, si bien la figura 1 representa el sistema para autorizar el acceso a un entorno de acceso controlado 100 con respecto a un dispositivo móvil 101a y a un dispositivo informático 101b del usuario y a un dispositivo informático remoto 102, se debe comprender que cualquier cantidad de dichos dispositivos puede interactuar con el sistema en la manera descrita en el presente documento. Se debe tener en cuenta, asimismo, que, aunque la figura 1 representa un sistema 100 con respecto al usuario 124, se debe comprender que cualquier cantidad de usuarios puede interactuar con el sistema de la manera descrita en el presente documento.

Se debe comprender, además, que, si bien los diversos dispositivos informáticos y máquinas a los que se hace referencia en el presente documento, incluidos, pero sin estar limitados a los mismos, el dispositivo móvil 101a y el servidor 105 del sistema y el dispositivo informático remoto 102, se conocen en el presente documento como dispositivos y/o máquinas individuales / únicas, en ciertas implementaciones los dispositivos y máquinas a los que se hace referencia, y sus operaciones, características y/o funcionalidades asociadas y/o adjuntas pueden ser combinados o dispuestos o empleados de otra manera en cualquier número de dichos dispositivos y/o máquinas, tal como a través de una conexión de red o conexión por cable, tal como es conocido por los expertos en la técnica.

Se debe comprender, asimismo, que los sistemas y métodos a modo de ejemplo descritos en el presente documento en el contexto del dispositivo móvil 101a no están específicamente limitados al dispositivo móvil, y pueden ser implementados utilizando otros dispositivos informáticos habilitados (por ejemplo, el dispositivo informático 102b del usuario).

En referencia a la figura 2A, el dispositivo móvil 101a a modo de ejemplo para ser utilizado con el sistema para autorizar el acceso a un entorno de acceso controlado 100, incluye diversos componentes de hardware y software que sirven para permitir el funcionamiento del sistema, incluidos uno o más procesadores 110, una memoria 120, un micrófono 125, un visualizador 140, una cámara 145, una salida de audio 155, un almacén 190 y una interfaz de comunicación 150. El procesador 110 sirve para ejecutar una aplicación de cliente en forma de instrucciones de software que pueden ser cargadas en la memoria 120. El procesador 110 puede estar formado por varios procesadores, una unidad de procesamiento central, CPU (Central Processing Unit, en inglés), una unidad de procesamiento de gráficos, GPU (Graphics Processing Unit, en inglés), un núcleo de múltiples procesadores o algún otro tipo de procesador, dependiendo de la implementación concreta.

Preferiblemente, la memoria 120 y/o el almacén 190 son accesibles por el procesador 110, permitiendo de este modo que el procesador reciba y ejecute instrucciones codificadas en la memoria y/o en el almacén para hacer que el dispositivo móvil y sus diversos componentes de hardware lleven a cabo operaciones para ciertos aspectos de los sistemas y métodos, tal como se describirá con mayor detalle a continuación. La memoria puede ser, por ejemplo, una memoria de acceso aleatorio (RAM - Random Access Memory, en inglés) o cualquier otro medio de almacenamiento legible por ordenador, volátil o no volátil, adecuado. Además, la memoria puede ser fija o extraíble. El almacén 190 puede adoptar diversas formas, dependiendo de la implementación concreta. Por ejemplo, el almacén puede contener uno o más componentes o dispositivos tales como un disco duro, una memoria rápida, un disco óptico regrabable, una cinta magnética regrabable, o alguna combinación de los anteriores. El almacén también puede ser fijo o extraíble.

Uno o más módulos 130 de software están codificados en el almacén 190 y/o en la memoria 120. Los módulos 130 de software pueden comprender uno o más programas o aplicaciones de software que tienen código de programa informático o un conjunto de instrucciones (conocidos como “la aplicación de cliente de autenticación de móvil”) ejecutada en el procesador 110. Tal como se representa en la figura 2B, preferiblemente, incluido entre los módulos de software 130 está dispuesto un módulo de interfaz de usuario 170, un módulo de captura biométrica 172, un módulo de análisis 174, un módulo de inscripción 176, un módulo de base de datos 178, un módulo de autenticación 180 y un módulo de comunicación 182, que son ejecutados por el procesador 110. Dicho código de programa informático o instrucciones configuran el procesador 110 para llevar a cabo operaciones de los sistemas y métodos descritos en la presente memoria, y pueden estar escritos en cualquier combinación de uno o más lenguajes de programación.

El código de programa puede ser ejecutado completamente en el dispositivo móvil 101, como un paquete de software independiente, en parte en el dispositivo móvil, en parte en el servidor 105 del sistema, o completamente en el servidor del sistema o en otro ordenador / dispositivo remoto. En este último escenario, el ordenador remoto puede estar conectado al dispositivo móvil 101 a través de cualquier tipo de red, incluida una red de área local (LAN - Local Area Network, en inglés) o una red de área amplia (WAN - Wide Area Network, en inglés), una red de comunicaciones móviles, una red celular, o la conexión puede ser realizada hasta un ordenador externo (por ejemplo, a través de Internet utilizando un proveedor de servicios de Internet).

Asimismo, se puede decir que el código de programa de los módulos de software 130 y uno o más dispositivos de almacenamiento legibles por ordenador (tales como la memoria 120 y/o el almacén 190) forman un producto de programa informático que puede ser fabricado y/o distribuido de acuerdo con la presente invención, como es conocido para los expertos de nivel medio en la técnica.

Se debe comprender que, en algunas realizaciones ilustrativas, uno o más de los módulos de software 130 pueden ser descargados a través de una red al almacén 190 desde otro dispositivo o sistema a través de la interfaz de comunicación 150 para su utilización dentro del sistema que autoriza el acceso a un entorno de acceso controlado 100. Además, se debe tener en cuenta que otra información y/o datos relevantes para el funcionamiento de los sistemas y métodos actuales (tales como la base de datos 185) también pueden ser almacenados en el almacén. Preferiblemente, dicha información se almacena en un almacén de datos cifrados que está asignado específicamente para almacenar de manera segura la información recopilada o generada por el procesador que ejecuta la aplicación de autenticación segura. Preferiblemente, las medidas de cifrado se utilizan para almacenar la información localmente en el almacén del dispositivo móvil y transmitir información al servidor 105 del sistema. Por ejemplo, dichos datos pueden ser cifrados utilizando un cifrado polimórfico de 1024 bits o, dependiendo de los controles de exportación, un método de cifrado de 256 bits, AES (Estándar de cifrado avanzado - Advanced Encryption Standard, en inglés). Además, el cifrado se puede llevar a cabo utilizando una clave remota (semillas) o claves locales (semillas). Se pueden utilizar métodos de cifrado alternativos como comprenderían los expertos en la técnica, por ejemplo, SHA256.

Además, los datos almacenados en el dispositivo móvil 101a y/o en el servidor 105 del sistema pueden ser cifrados utilizando la información biométrica, la información de vitalidad o la información del dispositivo móvil del usuario como clave de cifrado, por ejemplo, mediante la utilización de una función de derivación de clave se pueden generar una o más claves secretas a partir de información de usuario única, tal como la información biométrica. Por lo tanto, el par de claves está asociado de manera única con el usuario en virtud de estar derivadas de la información biométrica del usuario.

En algunas implementaciones, se puede utilizar una combinación de lo anterior para crear una clave única y compleja para el usuario que puede ser cifrada utilizando criptografía de curva elíptica, preferiblemente de al menos 384 bits de longitud, y ser almacenada en el dispositivo móvil. Además, esa clave se puede utilizar para proteger los datos del usuario almacenados en el dispositivo móvil y/o en el servidor del sistema.

También, preferiblemente, almacenada en el almacén 190, está dispuesta la base de datos 185. Tal como se describirá con mayor detalle a continuación, la base de datos contiene y/o mantiene diversos elementos de datos y elementos que se utilizan en las diversas operaciones del sistema 100 y el método para autenticar a un usuario. La información almacenada en la base de datos puede incluir, entre otros, un perfil de usuario, tal como se describirá con mayor detalle en el presente documento. Cabe señalar que, aunque la base de datos se describe como configurada localmente para el dispositivo móvil 101a, en ciertas implementaciones, la base de datos y/o diversos elementos de datos almacenados en la misma pueden, además o alternativamente, estar ubicados de manera remota (tal como en un dispositivo remoto 102 o un servidor 105 del sistema - no mostrado) y estar conectados al dispositivo móvil a través de una red de una manera conocida por los expertos de nivel medio en la técnica.

Una interfaz de usuario 115 también está operativamente conectada al procesador. La interfaz puede ser un dispositivo o dispositivos de entrada o salida, tales como un conmutador o conmutadores, un botón o botones, una tecla o teclas, una pantalla táctil, micrófono, etc., tal como se comprendería en la técnica de los dispositivos informáticos electrónicos. La interfaz de usuario sirve para facilitar la captura de comandos del usuario, tales como comandos de encendido / apagado o información del usuario y configuraciones relacionadas con la operación del sistema 100 para autenticar a un usuario. Por ejemplo, la interfaz sirve para facilitar la captura de cierta información del dispositivo móvil 101, tal como la información personal del usuario para inscribirse en el sistema a fin de crear un perfil de usuario.

El dispositivo informático 101a también puede incluir un visualizador 140 que está conectado, asimismo, operativamente, al procesador 110 del procesador. El visualizador incluye una pantalla o cualquier otro dispositivo de presentación de este tipo que permite al sistema dar indicaciones o proporcionar comentarios al usuario sobre el funcionamiento del sistema 100 para autenticar a un usuario. A modo de ejemplo, el visualizador puede ser un visualizador digital, tal como un visualizador de matriz de puntos u otro visualizador bidimensional.

A modo de ejemplo adicional, la interfaz y el visualizador pueden estar integrados en un visualizador de pantalla táctil. En consecuencia, el visualizador también se utiliza para mostrar una interfaz gráfica de usuario, que puede mostrar diversos datos y proporcionar “formularios” que incluyen campos que permiten la introducción de información por parte del usuario. Al tocar la pantalla táctil en ubicaciones correspondientes al visualizador de una interfaz gráfica de usuario, la persona puede interactuar con el dispositivo para introducir datos, cambiar configuraciones, funciones de control, etc. Por lo tanto, cuando se toca la pantalla táctil, la interfaz de usuario comunica este cambio al procesador, y la configuración se puede cambiar, o la información introducida por el usuario puede ser capturada y almacenada en la memoria.

El dispositivo móvil 101a incluye, asimismo, una cámara 145 capaz de capturar imágenes digitales. La cámara

puede estar formada por uno o más dispositivos de obtención de imágenes configurados para capturar imágenes de al menos una parte del cuerpo del usuario, incluidos los ojos y/o la cara del usuario mientras utiliza el dispositivo móvil 101a. La cámara sirve para facilitar la captura de imágenes del usuario para el análisis de imágenes por parte del procesador del dispositivo móvil que ejecuta la aplicación de autenticación segura, que incluye la identificación de características biométricas para autenticar (de manera biométrica) al usuario a partir de las imágenes. El dispositivo móvil 101a y/o la cámara 145 pueden incluir, asimismo, uno o más emisores de luz o señal (no mostrados), por ejemplo, un emisor de luz visible y/o un emisor de luz infrarroja y similares. La cámara puede estar integrada en el dispositivo móvil, tal como una cámara delantera o trasera que incorpora un sensor, por ejemplo y sin limitación, un sensor de CCD o de CMOS. Alternativamente, la cámara puede ser externa al dispositivo móvil 101a. Los expertos en la técnica comprenderán las posibles variaciones de la cámara y los emisores de luz. Además, el dispositivo móvil puede incluir, asimismo, uno o más micrófonos 104 para capturar grabaciones de audio, tal como comprenderían los expertos en la técnica.

Asimismo, la salida de audio 155 está conectada operativamente al procesador 110. La salida de audio puede ser cualquier tipo de sistema de altavoces que esté configurado para reproducir archivos electrónicos de audio, tal como comprenderían los expertos en la técnica. La salida de audio puede estar integrada en el dispositivo móvil 101, o ser externa al dispositivo móvil 101.

Diversos dispositivos / sensores 160 de hardware están conectados, asimismo, operativamente al procesador. Los sensores 160 pueden incluir: un reloj incorporado, para realizar un seguimiento de la hora del día, etc.; un dispositivo habilitado con GPS, para determinar la ubicación del dispositivo móvil; un acelerómetro, para realizar un seguimiento de la orientación y aceleración del dispositivo móvil; un magnetómetro de gravedad; sensores de proximidad; sensores de radiación de radiofrecuencia y otros dispositivos, tales como los comprendidos por los expertos en la técnica.

Una interfaz 150 de comunicación está conectada, asimismo, operativamente, al procesador 110, y puede ser cualquier interfaz que permita la comunicación entre el dispositivo móvil 101a y dispositivos, máquinas y/o elementos externos, tales como el servidor del sistema 105. Preferiblemente, la interfaz de comunicación incluye, pero no está limitada a, un módem, una tarjeta de interfaz de red (NIC - Network Interface Card, en inglés), una interfaz de red integrada, un transmisor/receptor de radiofrecuencia (por ejemplo, Bluetooth, celular, NFC), un transmisor/receptor de comunicación por satélite, un puerto de infrarrojos, una conexión USB y/o cualquier otra interfaz similar para conectar el dispositivo móvil a otros dispositivos informáticos y/o redes de comunicación, tales como las redes privadas e Internet. Dichas conexiones pueden incluir una conexión por cable o una conexión inalámbrica (por ejemplo, utilizando el estándar 802.11), aunque se debe comprender que la interfaz de comunicación puede ser prácticamente cualquier interfaz que permita la comunicación hacia/desde el dispositivo móvil.

En diversos puntos durante el funcionamiento del sistema que autoriza el acceso a un entorno de acceso controlado 100, el dispositivo móvil 101a se puede comunicar con uno o más dispositivos informáticos, tales como el servidor 105 del sistema, el dispositivo informático 101b del usuario y/o el dispositivo informático remoto 102. Dichos dispositivos informáticos transmiten y/o reciben datos hacia / desde el dispositivo móvil 101a, iniciando de este modo, preferiblemente, el mantenimiento y/o la mejora del funcionamiento del sistema 100, tal como se describirá con mayor detalle a continuación.

La figura 2C es un diagrama de bloques que ilustra una configuración a modo de ejemplo del servidor 105 del sistema. El servidor 105 del sistema puede incluir un procesador 210, que está conectado operativamente a diversos componentes de hardware y software que sirven para permitir el funcionamiento del sistema 100 para facilitar la autenticación segura de transacciones en un terminal. El procesador 210 sirve para ejecutar instrucciones para realizar diversas operaciones relacionadas con la autenticación del usuario y el procesamiento de transacción, tal como se describirá con mayor detalle a continuación. El procesador 210 puede estar formado por varios procesadores, un núcleo de múltiples procesadores o algún otro tipo de procesador, dependiendo de la implementación concreta.

Preferiblemente, la memoria 220 y/o un medio de almacenamiento 290 son accesibles por el procesador 210, permitiendo de este modo que el procesador 210 reciba y ejecute instrucciones almacenadas en la memoria 220 y/o en el almacén 290. La memoria 220 puede ser, por ejemplo, una memoria de acceso aleatorio (RAM) o cualquier otro medio de almacenamiento legible por ordenador, volátil o no volátil, adecuado. Además, la memoria 220 puede ser fija o extraíble. El almacén 290 puede adoptar diversas formas, dependiendo de la implementación concreta. Por ejemplo, el almacén 290 puede contener uno o más componentes o dispositivos tales como un disco duro, una memoria rápida, un disco óptico regrabable, una cinta magnética regrabable, o alguna combinación de los anteriores. El almacén 290 también puede ser fijo o extraíble.

Uno o más módulos de software 130 (representados en la figura 2B) están codificados en el almacén 290 y/o en la memoria 220. Los módulos de software 130 pueden comprender uno o más programas o aplicaciones de software (conocidos conjuntamente como (“aplicación de servidor de autenticación segura”) que contienen código de programa informático o un conjunto de instrucciones ejecutadas en el procesador 210. Dicho código de programa informático o instrucciones para llevar a cabo operaciones e implementar aspectos de los sistemas y métodos descritos en la presente memoria pueden estar escritos en cualquier combinación de uno o más lenguajes de

programación, tal como comprenderían los expertos en la técnica. El código del programa puede ser ejecutado completamente en el servidor 105 del sistema como un paquete de software independiente, en parte en el servidor 105 del sistema y en parte en un dispositivo informático remoto, tal como un dispositivo informático remoto 102, un dispositivo móvil 101a y/o un dispositivo informático 101b del usuario, o completamente en dichos dispositivos informáticos remotos. Tal como se representa en la figura 2B, preferiblemente, incluido entre los módulos de software 130 están dispuestos en un módulo de análisis 274, un módulo de inscripción 276, un módulo de autenticación 280, un módulo de base de datos 278 y un módulo de comunicación 282, que son ejecutados por el procesador 210 del servidor del sistema.

Asimismo, preferiblemente almacenada en el almacén 290 está dispuesta una base de datos 280. Tal como se describirá con mayor detalle a continuación, la base de datos 280 contiene y/o mantiene varios elementos de datos y elementos que se utilizan a lo largo de las diversas operaciones del sistema 100, incluidos, entre otros, los perfiles de usuario como se describirán con mayor detalle en el presente documento. Cabe señalar que, aunque la base de datos 280 se representa como configurada localmente para el dispositivo informático 205, en ciertas implementaciones, la base de datos 280 y/o diversos elementos de datos almacenados en la misma pueden estar almacenados en una memoria legible por ordenador o en un medio de almacenamiento que esté ubicado de manera remota y conectado al servidor 105 del sistema a través de una red (no mostrada), de una manera conocida por los expertos en la técnica.

Una interfaz de comunicación 255 está operativamente conectada, asimismo, al procesador 210. La interfaz de comunicación 255 puede ser cualquier interfaz que permita la comunicación entre el servidor 105 del sistema y dispositivos, máquinas y/o elementos externos. Preferiblemente, la interfaz 255 de comunicación incluye, pero no está limitada limita a, un módem, una tarjeta de interfaz de red (NIC), una interfaz de red integrada, un transmisor/receptor de radiofrecuencia (por ejemplo, Bluetooth, celular, NFC), un transmisor/receptor de comunicación por satélite, un puerto de infrarrojos, una conexión USB y/o cualquier otra interfaz similar para conectar el dispositivo informático 205 a otros dispositivos informáticos y/o redes de comunicación, tales como redes privadas e Internet. Dichas conexiones pueden incluir una conexión por cable o una conexión inalámbrica (por ejemplo, utilizando el estándar 802.11), aunque se debe comprender que la interfaz de comunicación 255 puede ser prácticamente cualquier interfaz que permita la comunicación hacia/desde el procesador 210.

El funcionamiento del sistema para autorizar el acceso a un entorno de acceso controlado y los diversos elementos y componentes descritos anteriormente se apreciarán adicionalmente con referencia al método para autenticar a un usuario tal como se describe a continuación, junto con las figuras 3 y 4 siguiendo con la referencia a las figuras 1 y 2A a 2C. Los procesos representados en las figuras 3 y 4 se muestran desde la perspectiva del dispositivo móvil 101a, así como del servidor 105 del sistema; no obstante, se debe comprender que los procesos pueden ser llevados a cabo, en su totalidad o en parte, por el dispositivo móvil 101a, el servidor 105 del sistema y/u otros dispositivos informáticos (por ejemplo, el dispositivo informático remoto 102 y/o el dispositivo informático 101b del usuario) o cualquier combinación de los anteriores. Se debe apreciar que se pueden realizar más o menos operaciones de las que se muestran en las figuras y se describen en el presente documento. Estas operaciones pueden ser llevadas a cabo, asimismo, en un orden diferente al descrito en el presente documento. También se debe comprender que una o más de las etapas pueden ser llevadas a cabo por el dispositivo móvil 101a y/o en otros dispositivos informáticos (por ejemplo, el dispositivo informático 101b, el servidor 105 del sistema y el dispositivo informático remoto 102).

La figura 3 es un diagrama de flujo que ilustra una rutina 400 para inscribir al usuario 124 con el sistema 100. El proceso de inscripción verifica la identidad del usuario para garantizar que el usuario es quien dice ser y también puede especificar la manera en que el usuario 124 y el dispositivo móvil 101a se identifican con el servidor 105 del sistema. Además, la inscripción puede crear un perfil de usuario que asocie al usuario 124 con los dispositivos del usuario (por ejemplo, el dispositivo móvil del usuario 101a y/o el dispositivo informático 101b del usuario) y con una o más de las cuentas de transacción del usuario. La inscripción incluye, asimismo, capturar (por ejemplo, leer) las características biométricas del usuario, generar uno o más identificadores biométricos que caracterizan esas características y determinar la vitalidad del usuario. Estas etapas pueden ser llevadas a cabo para la verificación, así como para establecer una línea de base para futuras sesiones de verificación, tal como se describe más adelante en el presente documento. Por consiguiente, se puede apreciar que muchas de las etapas explicadas en relación con la figura 3 se pueden llevar a cabo durante las sesiones de autenticación de usuario posteriores, tal como se describe en relación con la figura 4.

El proceso comienza en la etapa 305, en la que se establece una sesión de comunicación inicial entre el dispositivo móvil 101a y el servidor 105 del sistema. En algunas implementaciones, las comunicaciones entre el dispositivo móvil y el servidor del sistema se pueden establecer utilizando capas de puertos seguros (SSL - Secure Socket Layers) de dos direcciones establecidas en una comunicación de SSL de una dirección. De manera más específica, el procesador 110 del dispositivo móvil, que se configura ejecutando una o más aplicaciones de software, que incluyen, preferiblemente, el módulo de comunicación 182 y el módulo de inscripción 176, puede transmitir una llamada de API al servidor 105 del sistema y establecer una sesión de comunicación de SSL de una dirección con el servidor 105 del sistema para cifrar las comunicaciones. La llamada de API puede incluir, asimismo, una clave de SSL privada de dos direcciones para establecer un entorno de comunicación seguro de SSL de dos direcciones. En algunas implementaciones, el dispositivo móvil puede transmitir un certificado de SSL de dos direcciones precargado

y una clave de API que es exclusiva de la aplicación de cliente del dispositivo móvil. El certificado y la clave precargados pueden ser instancias de una sola utilización que son almacenados cuando la aplicación de cliente se almacena en la memoria.

Además, en la etapa 305, el procesador 110 del dispositivo móvil, que se configura ejecutando instrucciones en forma de uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de inscripción 176, el módulo de captura 172, el módulo de comunicación 182, el módulo de base de datos 178 y el módulo de análisis 174, también puede inicializar los diversos componentes del dispositivo móvil 101a y determinar su operatividad y capacidades respectivas.

La inicialización se puede realizar durante el proceso de inscripción inicial, y también se puede realizar durante los siguientes procesos de captura / autenticación biométrica. Sin embargo, se debe comprender que algunas o todas las etapas no necesitan ser llevadas a cabo con cada inicialización, y pueden ser llevadas a cabo en la inscripción inicial y/o periódicamente, a continuación. A modo de ejemplo no limitativo, la inscripción del usuario y la inicialización de un dispositivo móvil para facilitar la autenticación biométrica utilizando un dispositivo móvil se describen en el presente documento y en la Solicitud de Patente de los Estados Unidos de Nº de serie 61/842.800, en tramitación con la presente y comúnmente asignada.

A continuación, en la etapa 310, el dispositivo móvil 101a recoge información de identificación del usuario. De manera más específica, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de inscripción 176 y el módulo de interfaz de usuario 170, puede solicitar al usuario que introduzca la información de identificación del usuario y reciba las entradas del usuario a través de la interfaz de usuario 115. La información de identificación del usuario puede incluir información sobre la identidad del usuario (por ejemplo, nombre, dirección, número de la seguridad social, etc.). Por ejemplo, tal como se muestra en la figura 6A, el visualizador 600 del dispositivo móvil puede solicitar al usuario que introduzca dicha información personal sobre la identidad del usuario 610. En algunas implementaciones, una parte o la totalidad de la información se puede recopilar de manera automática de la memoria del dispositivo móvil 101a o de un dispositivo informático remoto.

Además, la información de identificación del usuario puede incluir información sobre una o más cuentas de transacción con las que el usuario desea acceder a uno o más ACE de acuerdo con los sistemas y métodos descritos en el presente documento. Por ejemplo, el usuario puede introducir el inicio de sesión preexistente y las contraseñas 615 asociadas con las diversas cuentas de transacción del usuario (por ejemplo, cuentas bancarias en línea, inicios de sesión en sitios web, cuentas VPN y similares) o números de cuenta 620 de transacción reales (por ejemplo, números de cuenta bancaria, números de encaminamiento, números de tarjeta de débito / crédito, fechas de vencimiento y similares) tal como se muestra en la figura 6A. En algunas implementaciones, el procesador de dispositivo móvil configurado y/o el servidor 105 del sistema pueden obtener de manera automática una parte o la totalidad de dicha información directamente de las organizaciones empresariales asociadas con las cuentas de transacción y/o los ACE después de verificar la identidad del usuario de acuerdo con la información de identificación del usuario proporcionada por el usuario.

A continuación, en la etapa 315, se recopila información de identificación del dispositivo móvil. La información de identificación del dispositivo móvil puede incluir, entre otros, al menos una parte del ID del dispositivo, ID del sistema Android, IMEI, número de serie de la CPU, número de serie de la GPU y otros identificadores similares que son exclusivos para el dispositivo móvil. De manera más específica, el procesador del dispositivo móvil 110, que se configura ejecutando uno o más módulos de software 130, incluido, preferiblemente, el módulo de inscripción 176, puede consultar a los diversos componentes de hardware y software del dispositivo móvil 101a para obtener información de identificación del dispositivo respectivo. Utilizando la información de identificación del dispositivo móvil, el procesador del dispositivo móvil configurado o el servidor del sistema pueden generar uno o más identificadores de dispositivo móvil que identifican de manera única el dispositivo móvil, tal como se describe más adelante en el presente documento.

A continuación, en la etapa 320, se verifica la identidad del usuario. La verificación de identidad proporciona seguridad adicional y determina que el usuario 124 es, realmente, quien dice ser. Se debe comprender que la verificación de la identidad del usuario puede ser llevada a cabo por el servidor 105 del sistema, por el dispositivo móvil 101a o por una combinación de los anteriores.

Por ejemplo y sin limitación, el procesador del dispositivo móvil 110, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de inscripción 176 y el módulo de comunicación 182, puede transmitir la información de identificación del usuario al servidor 105 del sistema para verificación de identidad. En algunas implementaciones, el servidor 105 del sistema puede consultar una base de datos que almacena los datos personales del usuario y determinar si la información del usuario corresponde a los datos almacenados previamente. Si la información comparada no corresponde en un grado suficiente o se requiere una entrada adicional del usuario, el servidor del sistema también puede generar preguntas de seguimiento que son específicas para el usuario de acuerdo con la base de datos de datos personales, y enviar las preguntas al dispositivo móvil 101a solicitando, por lo tanto, al usuario 124 que introduzca respuestas a las preguntas utilizando el dispositivo móvil. Los expertos en la técnica comprenderán diversos métodos para verificar la identidad de un

usuario.

Además o alternativamente, la verificación de identidad también se puede realizar de acuerdo con la información del dispositivo móvil, tal como se describe adicionalmente en el presente documento. Por ejemplo, mediante la determinación, por el servidor 105 del sistema, de si la información del usuario y la información del dispositivo corresponden a la cuenta del servicio de comunicación móvil asociada con el dispositivo móvil 101a tal como se obtiene del sistema corporativo del proveedor del servicio de telefonía móvil.

En algunas implementaciones, el servidor 105 del sistema puede verificar la identidad del usuario de acuerdo con la información de la cuenta de transacción y con la contraseña que ya está asociada con una o más cuentas de transacción existentes asociadas con el usuario y almacenadas en el servidor del sistema o en un almacén de datos seguro que es accesible por el servidor del sistema. Por ejemplo, si el servidor del sistema está integrado con un sistema de seguridad corporativo existente, el usuario se puede identificar mediante, por ejemplo, un número de cuenta y un número de pin existentes o un inicio de sesión y contraseña. Además o alternativamente, la identidad del usuario puede ser verificada utilizando servicios de verificación de terceros, por ejemplo, el sistema de verificación de información personal Acxiom, comercializado por la firma Acxiom Corp. de Little Rock, Arkansas.

Se debe comprender que la rigurosidad de la verificación de identidad puede variar dependiendo del nivel de seguridad, según lo dicte la implementación particular del sistema 100 de autenticación seguro. Por ejemplo, el inicio de sesión del usuario en un foro / mesa redonda en línea puede requerir solo una verificación liberal de la identidad del usuario, mientras que las aplicaciones en las que se utilizan los sistemas y métodos dados a conocer para autenticar una transacción financiera pueden requerir una validación estricta de la identidad. De este modo, la verificación de identidad puede variar desde una verificación estricta, utilizando servicios tales como Axciom, hasta, simplemente, confirmación de si el inicio de sesión y la contraseña del usuario coinciden con un inicio de sesión y contraseña existentes.

A continuación, en la etapa 325, si se verifica la identidad de un usuario, se puede generar y almacenar un perfil de usuario. El perfil del usuario puede incluir uno o más fragmentos de información de identificación del usuario e identificación del dispositivo móvil. Además, el perfil del usuario puede incluir información relacionada con una o más cuentas de transacción del usuario, así como configuraciones que pueden ser utilizadas para guiar el funcionamiento del sistema 100 según las preferencias del usuario.

En algunas implementaciones, el servidor 105 del sistema puede generar un identificador único para el usuario (un “ID de usuario”) y un identificador de dispositivo móvil asociado (un “ID de dispositivo móvil”) y almacenar los identificadores en un entorno persistente en grupo para crear el perfil para el usuario. El ID de usuario y el ID del dispositivo móvil se pueden generar utilizando uno o más fragmentos de la información de identificación del usuario y la información de identificación del dispositivo móvil, respectivamente. Se debe comprender que una información de identificación de usuario y una información de identificación de dispositivo móvil adicionales se pueden almacenar, asimismo, para crear el perfil de usuario, o almacenarse en asociación con el perfil de usuario.

Además, el ID de usuario y el ID del dispositivo móvil asociado se pueden almacenar en asociación con información relativa a una o más cuentas de transacción descritas en la etapa 315. En algunas implementaciones, la información de la cuenta de transacción específica se puede almacenar en el servidor 105 del sistema, permitiendo de este modo que el servidor del sistema autorice la totalidad o una parte de las transacciones solicitadas en nombre del usuario y de la organización empresarial. Además o alternativamente, el perfil de usuario se puede asociar con una cuenta de transacción utilizando, por ejemplo, un identificador (por ejemplo, un ID de sitio o un identificador único global, etc.) u otro puntero a un almacén de datos seguro que almacena la información confidencial de la cuenta de transacción, digamos, el dispositivo informático remoto 102 operado por una organización empresarial. En consecuencia, no se requiere que el servidor 105 del sistema almacene información confidencial de la cuenta de transacción y, tal como se describe más adelante en el presente documento, el servidor 105 del sistema puede generar y/o enviar solicitudes para autorizar a un usuario a la organización empresarial apropiada para su posterior procesamiento. Además o alternativamente, el servidor del sistema puede consultar el almacén de datos seguro para recopilar la información necesaria para procesar dichas solicitudes.

En este momento, se puede apreciar que el ID del usuario se puede utilizar para asignar el perfil del usuario a las cuentas de transacción heredadas del usuario. Además, el ID del dispositivo móvil vincula el dispositivo a un perfil de usuario. En algunas implementaciones, los ID de usuario son una convención, mientras que los ID de dispositivo móvil son obligatorios, porque solo el ID del dispositivo móvil puede vincular el par de usuario 124 y dispositivo móvil 101a con el perfil del usuario guardado en el servidor 105 del sistema y/o las cuentas de transacción del usuario. Además, cualquier información adicional incluida en el perfil del usuario puede ser utilizada con el propósito de no repudio o procedencia por parte del servidor 105 del sistema en futuras solicitudes de autorización.

Se puede apreciar que los perfiles de usuario pueden ser creados por el servidor 105 del sistema y/o el dispositivo móvil 101a. Además, una o más instancias de un perfil de usuario pueden estar almacenadas en diversos dispositivos (por ejemplo, el servidor del sistema 105, el dispositivo móvil 101a, el dispositivo informático remoto 102 o el dispositivo informático 101b del usuario). Además, la información incluida en las diversas instancias de los perfiles del usuario puede variar de un dispositivo a otro. Por ejemplo, una instancia del perfil del usuario que está

almacenada en el dispositivo móvil 101a puede incluir el ID de usuario, el ID del dispositivo móvil, la información de identificación del usuario y la información confidencial relativa a las cuentas de transacción del usuario, por ejemplo, números de cuenta y similares. A modo de ejemplo adicional, la instancia del perfil del usuario almacenada por el servidor 105 del sistema puede incluir el ID del usuario, el ID del dispositivo móvil, otros identificadores exclusivos asignados al usuario, e información que identifica las cuentas de transacción del usuario, pero no incluye información confidencial de la cuenta.

En algunas implementaciones, la generación del perfil del usuario por parte del servidor 105 del sistema puede incluir, asimismo, la generación de una clave privada, por ejemplo, un certificado de SSL en dos direcciones, exclusivo, que utiliza la información de identificación del usuario, que puede incluir la información relativa a la cuenta o cuentas de transacción del usuario, y la información de identificación del dispositivo móvil. La clave privada generada puede ser transmitida, asimismo, de vuelta al dispositivo móvil 101a, para su almacenamiento en el dispositivo móvil. En consecuencia, la clave generada puede ser utilizada para comunicaciones posteriores junto con sesiones de afirmación de identidad.

Por ejemplo, la fase de inscripción / génesis puede vincular la información que identifica al usuario (por ejemplo, el ID del usuario, el SSN, el correo electrónico u otros identificadores de usuario) a un nombre común (CN - Common Name, en inglés) que puede ser la forma particular en que el usuario concreto es identificado de manera única por el servidor 105 del sistema y/o los sistemas de cuentas de transacción heredadas en la clave de capas de conector seguro de dos direcciones. En consecuencia, la fase de génesis puede vincular, asimismo, cuentas de transacción heredadas asociadas con el usuario (por ejemplo, la cuenta bancaria del usuario) con la identidad del usuario guardada en el servidor 105 del sistema.

La clave privada es generada en el servidor 105 del sistema y vincula el par de dispositivo móvil 101a (por ejemplo, el ID del dispositivo móvil) y usuario (por ejemplo, el ID del usuario) a la identidad del usuario (por ejemplo, el identificador del usuario, el nombre común, etc.) que se utilizará para una comunicación posterior

La identidad, tal como se afirma a través de la clave de capa de conector seguro de dos direcciones se puede mantener para toda comunicación. Esta clave está codificada con una contraseña conocida solo por el dispositivo que se utiliza durante la inscripción, que, en el presente ejemplo, es el dispositivo móvil 101a. Además, la clave es colocada, mediante programación, en el almacén de claves en el dispositivo móvil 101a. Es el único mecanismo que permite la identidad y los enlaces a las fases de génesis. Ningún humano o dispositivo conoce la contraseña utilizada para cifrar la clave de la SSL de dos direcciones. En consecuencia, el dispositivo móvil 101a, que utiliza la clave privada, tiene una identidad que ofrecer en comunicaciones posteriores. Se puede apreciar que cada dispositivo móvil habilitado asociado con un usuario puede tener una clave única que se puede vincular al mismo perfil de usuario, que permite la utilización de múltiples dispositivos de la misma manera. Además o alternativamente, se pueden establecer y mantener perfiles de usuario separados para cada par de usuario y dispositivo de manera independiente o vinculada. También se puede apreciar que, de manera similar, múltiples usuarios pueden utilizar el mismo o los mismos dispositivos que corresponden a perfiles de usuario individuales o a perfiles de usuario conjuntos o a perfiles de usuario vinculados de otro modo.

En consecuencia, como resultado de la génesis / inscripción, se crea un perfil de usuario que asocia al usuario 124, el dispositivo móvil 101a y una o más cuentas de transacción. Además, al dispositivo móvil 101a se le puede proporcionar información (por ejemplo, un identificador de usuario y un identificador de dispositivo móvil exclusivos y/o claves exclusivas) para identificar al usuario 124 y al dispositivo móvil 101a en comunicaciones posteriores, por ejemplo, en sesiones de afirmación de identidad.

A continuación, en la etapa 330, se reciben las configuraciones del usuario. Las configuraciones incluyen preferencias y reglas definidas por el usuario para guiar la operación del sistema 100. En algunas implementaciones, durante el proceso de inscripción, o en cualquier momento posterior, el dispositivo móvil 101a puede solicitar al usuario que introduzca configuraciones y las asocie con una o más de las cuentas de transacción del usuario. La configuración puede ser almacenada por el dispositivo móvil o el servidor 105 del sistema, o por una combinación de los anteriores. En consecuencia, la configuración definida por el usuario puede hacer que el sistema 100 autentique al usuario y/o facilite las transacciones de manera automática, o con menos entradas del usuario.

En algunas implementaciones, la configuración de entrada del usuario puede especificar entornos de control de acceso preferidos a los que el usuario desea acceder utilizando el sistema. Por ejemplo, la configuración puede identificar ciertos sitios web o aplicaciones en las que el usuario desea iniciar sesión de manera automática utilizando el sistema 100. En algunas implementaciones, la configuración puede especificar circunstancias en las que un usuario desea autenticarse para obtener acceso a dichos entornos. Por ejemplo, el usuario desea autenticarse solo cuando realiza una compra a través de una aplicación móvil concreta, en lugar de autenticarse inmediatamente al iniciar la aplicación móvil concreta.

En algunas implementaciones, la configuración del usuario puede especificar preferencias para realizar transacciones. Por ejemplo y sin limitación, el usuario puede especificar métodos / cuentas de pago predeterminados configurando de este modo el dispositivo móvil 101a y/o el servidor 105 del sistema para seleccionar cuentas de transacción y/o procesar transacciones de manera eficiente. Además, el usuario puede

asociar los métodos de pago con vendedores especificados. A modo de ejemplo adicional, un usuario puede especificar reglas para controlar la utilización de ciertas cuentas de transacción, por ejemplo, haciendo que el servidor 105 del sistema impida ciertos tipos de transacciones, haga que se envíe una notificación al usuario o implemente medidas de seguridad adicionales para garantizar la utilización aprobada de la cuenta.

En algunas implementaciones, la configuración del usuario puede incluir reglas de acceso definidas por el usuario o configuraciones de privacidad que controlan el acceso a la información, actividad o cuentas del usuario. Por ejemplo, la configuración puede identificar a otros usuarios inscritos o a organizaciones empresariales en los que el usuario desea tener acceso a las cuentas del usuario o a la información asociada con el usuario.

En algunas implementaciones, la configuración puede especificar reglas de transacción predeterminadas para realizar transacciones con organizaciones empresariales definidas. Por ejemplo, la configuración puede especificar que el usuario habitualmente desea retirar una cantidad prescrita de efectivo de una cuenta de transacción predeterminada cuando realiza una transacción en un cajero automático. En consecuencia, el sistema 100 puede realizar la transacción de manera automática, aplicando las configuraciones definidas por el usuario cuando se inicia una transacción en un cajero automático sin requerir que el usuario proporcione o confirme la cuenta de la transacción y los detalles de la transacción.

En algunas implementaciones, un usuario puede establecer, asimismo, reglas de transacción únicas antes de realizar ciertas transacciones electrónicas. Por ejemplo, el usuario puede especificar que la siguiente vez que acceda a la red de una institución financiera, el usuario desea realizar un pago de 500 $ en la cuenta del usuario en la organización empresarial utilizando un método de pago concreto. De esta manera, el usuario puede poner en cola varias transacciones diferentes a realizar por el sistema 100 de manera automática.

Se debe comprender que las configuraciones descritas se presentan como ejemplos no limitativos, y que se puede utilizar una amplia variedad de configuraciones para controlar el funcionamiento del sistema 100 y cómo interactúan los usuarios con el sistema 100.

Asimismo, se debe comprender que, durante la inscripción y en cualquier momento posterior y al utilizar cualquier dispositivo de usuario (por ejemplo, un dispositivo móvil 101a y un dispositivo informático 101b del usuario) que esté inscrito en el sistema, el usuario puede ajustar la configuración con respecto a las preferencias del usuario para interactuar con el sistema 100. Por ejemplo, el dispositivo móvil puede recibir del usuario información adicional de identificación del usuario, contraseñas, información de cuenta de transacción y similares para el almacenamiento local en el dispositivo móvil 101a, en el servidor 105 del sistema, en el dispositivo informático 101b del usuario o en una combinación de los anteriores. De este modo, cualquiera de los dispositivos informáticos del sistema 100 puede ser configurado para que actúe como una plataforma para facilitar de manera automática el acceso a los ACE utilizando dichas cuentas de transacción, y para proporcionar la información del usuario a los diversos dispositivos informáticos habilitados (por ejemplo, un dispositivo móvil 101a, un dispositivo informático 101b del usuario, un dispositivo informático remoto 102).

A continuación, en la etapa 335, las características biométricas del usuario son capturadas utilizando el dispositivo móvil 101a. En algunas implementaciones, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de inscripción 176, el módulo de análisis 174, el módulo de interfaz de usuario 170 y el módulo de captura 172, solicita al usuario la captura de imágenes del iris / los iris del usuario, un ojo o los ojos, la región periocular, la cara (por ejemplo, la región de Vitruvio) o una combinación de lo anterior, utilizando la cámara 145 del dispositivo móvil, y almacena una secuencia de imágenes en el almacén 190 o la memoria 120.

En algunas implementaciones, el procesador 110 configurado también puede hacer que el micrófono 104 capture la voz del usuario a través de un micrófono en comunicación con el dispositivo móvil, y grabe los datos de audio en la memoria del dispositivo. Por ejemplo, se le puede solicitar al usuario que diga palabras o frases que son grabadas utilizando el micrófono. El dispositivo móvil también puede capturar imágenes de la cara, los ojos, etc. del usuario a la vez que graba la voz del usuario, o de manera separada.

A continuación, en la etapa 340, se generan uno o más identificadores biométricos a partir de la información biométrica capturada, y se almacenan para completar la etapa de inscripción. De manera más específica, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172, el módulo de base de datos 178, el módulo de análisis 174, puede analizar la información biométrica capturada por la cámara y generar un identificador biométrico (por ejemplo, “un identificador de Vitruvio”) tal como se describe adicionalmente en el presente documento y en referencia a la figura 5.

En algunas implementaciones, las características biométricas de la voz del usuario pueden ser caracterizadas como una impresión de voz, de modo que el usuario pueda autenticarse de manera biométrica a partir de las características de la voz del usuario de acuerdo con los algoritmos de identificación del origen de la voz. Por ejemplo, el componente de audio de la información biométrica del usuario puede ser analizado por el procesador del dispositivo móvil de acuerdo con los algoritmos de identificación del origen de la voz para crear una impresión de voz

para el usuario que pueda ser almacenada por el dispositivo móvil. Las diversas tecnologías utilizadas para procesar datos de voz, generar y almacenar impresiones de voz pueden incluir, sin limitación, estimación de frecuencia, modelos ocultos de Markov, modelos de mezcla gaussiana, algoritmos de coincidencia de patrones, redes neuronales, representación matricial, cuantificación vectorial y árboles de decisión. Por consiguiente, el usuario puede autenticarse / identificarse o determinar la vitalidad analizando las características de la voz del usuario de acuerdo con los algoritmos de identificación del origen de la voz conocidos tal como se describe adicionalmente en el presente documento.

En algunas implementaciones, el procesador 110 del dispositivo móvil configurado puede determinar si la información biométrica capturada es suficiente para generar identificadores biométricos adecuados. Si las características biométricas no se identifican con suficiente detalle de la información biométrica capturada (por ejemplo, imágenes, datos de audio, etc.), el procesador del dispositivo móvil configurado puede solicitar al usuario que repita el proceso de captura biométrica a través del visualizador o de otra salida similar del dispositivo móvil 101a. Además, el procesador 110 del dispositivo móvil configurado puede proporcionar una retroalimentación durante la captura y después de la misma, lo que sugiere un “escenario ideal”, por ejemplo y sin limitación, una ubicación con luz visible adecuada, la distancia y orientación apropiadas de la cámara en relación con la cara del usuario y similares.

Además, en algunas implementaciones, el procesador del dispositivo móvil configurado puede analizar la luz capturada por la cámara y el espectro de luz que pueden emitir los emisores de luz en el dispositivo móvil, y ajustar la frecuencia de la luz emitida durante la etapa de captura para mejorar la calidad de la información biométrica capturada por la cámara. Por ejemplo, si el procesador configurado no puede generar un identificador biométrico y determina que el usuario tiene ojos de color más oscuro, el procesador puede hacer que la cámara recupere los datos de la imagen y haga que el emisor de luz emita frecuencias de luz que son, digamos, lo más cerca posible del espectro infrarrojo, dadas las capacidades particulares del dispositivo móvil para capturar más características del iris del usuario.

Además de generar uno o más identificadores biométricos tal como se explicó anteriormente, el procesador del dispositivo móvil configurado también puede generar identificadores que incorporen múltiples instancias de uno o más identificadores biométricos. Por ejemplo, durante el proceso de inscripción, el procesador del dispositivo móvil configurado puede capturar y analizar múltiples secuencias de información biométrica para generar múltiples identificadores biométricos que, conjuntamente, son representaciones virtuales adecuadas del usuario 124 en las múltiples capturas (por ejemplo, para garantizar que el procesador configurado ha “obtenido” suficiente información biométrica para el usuario 124). En consecuencia, la parte de captura biométrica del proceso de inscripción se puede realizar varias veces en varios intervalos y ubicaciones, para capturar la información biométrica del usuario en varios escenarios del mundo real, lo que aumenta la probabilidad de que la futura autenticación sea positiva y sin errores. Se debe comprender que los múltiples identificadores biométricos pueden ser almacenados por separado y/o combinados en un solo identificador.

Además o alternativamente, se pueden generar identificadores biométricos complejos fusionando los identificadores generados de acuerdo con diferentes modalidades de identificación biométrica para crear un identificador biométrico multidimensional que es una representación biométrica combinada del usuario. Por ejemplo, el procesador del dispositivo móvil configurado ejecutando uno o más módulos que incluyen, preferiblemente, el módulo de análisis 174, puede combinar la impresión o impresiones de voz del usuario y el identificador o identificadores de Vitruvio.

En algunas implementaciones, los identificadores biométricos pueden ser almacenados localmente en el dispositivo móvil 101a en asociación con el perfil del usuario, de tal modo que el dispositivo móvil pueda realizar la autenticación biométrica de acuerdo con los identificadores biométricos. Además o alternativamente, los identificadores biométricos pueden ser almacenados en asociación con el perfil del usuario en un dispositivo informático remoto (por ejemplo, el servidor 105 del sistema o el dispositivo informático remoto 102), permitiendo que esos dispositivos lleven a cabo la autenticación biométrica del usuario.

En la etapa 345, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172, también puede recibir información basada en visión no artificial. La información basada en visión no artificial, en general, hace referencia a las características de comportamiento del usuario 124 durante la inscripción y a las sesiones de autenticación posteriores que son indicativas de la identidad del usuario, así como de la vitalidad del usuario. Por ejemplo, y sin limitación, la información basada en visión no artificial puede incluir una hora recibida de un reloj incorporado, una ubicación recibida del dispositivo GPS, a qué distancia de la cara del usuario está posicionada la cámara durante la captura de imágenes, calculada a partir de imágenes o de otros dispositivos de medición de proximidad incorporados, la orientación del dispositivo móvil y la aceleración del dispositivo móvil recibida desde un acelerómetro, la radiación de RF detectada por un detector de RF, magnetómetros de gravedad que detectan el campo magnético de la Tierra, para determinar la orientación tridimensional en la que está sujetado el teléfono, sensores de luz que miden los niveles de intensidad de luz y similares.

En algunas implementaciones, la información basada en visión no artificial es recibida a lo largo del tiempo y almacenada, de tal modo que el procesador configurado pueda determinar patrones en la información que son

exclusivos para el usuario 124 aplicando algoritmos de comportamiento, tal como comprenderían los expertos en la técnica. En consecuencia, durante las etapas de autenticación posteriores, los datos actuales basados en visión no de ordenador recopilados pueden ser analizados y comparados con los rasgos de comportamiento establecidos del usuario, para verificar la identidad del usuario y determinar si la información es indicativa de vitalidad. Por ejemplo, los patrones de comportamiento basados en el tiempo y la ubicación pueden ser identificados con el tiempo y la posición actual en comparación con el patrón para determinar si se muestra algún comportamiento anormal. A modo de ejemplo adicional, la "oscilación" o aceleración concretas del dispositivo móvil durante múltiples procesos de autenticación se puede caracterizar como un rasgo de comportamiento, y la oscilación particular de la autenticación actual puede ser comparada, para identificar un comportamiento anormal. A modo de ejemplo adicional, la orientación del dispositivo o la distancia desde la cara del usuario también pueden ser comparadas de manera similar. A modo de ejemplo adicional, se puede establecer una firma de radiación de RF para el usuario durante la inscripción, y compararla con mediciones futuras para identificar niveles anormales de radiación de RF (por ejemplo, sugiriendo la utilización de pantallas de video para suplantar la identidad para el sistema).

En la etapa 350, el procesador del dispositivo móvil configurado mediante la ejecución de uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de análisis 174, puede generar uno o más identificadores de vitalidad que caracterizan los datos biométricos del usuario capturado y/o la información basada en visión no artificial que son indicativos de la vitalidad del usuario. Tal como se señaló anteriormente, la determinación de la vitalidad es una medida anti-suplantación de identidad que puede ser llevada a cabo durante la inscripción y las sesiones de autenticación posteriores para garantizar que la secuencia de imágenes capturada por el dispositivo de imágenes sea de un sujeto vivo y no una representación visual del usuario, por ejemplo, mediante un video de alta resolución. En algunas implementaciones, la vitalidad se determina detectando el movimiento de las características biométricas, porque cada vez que el usuario se inscribe o valida, el usuario realmente se moverá un poco, sin importar lo estable esté tratando de ser.

En algunas implementaciones, el proceso para generar identificadores biométricos, tal como se explicó en la etapa 335 y el proceso 500 de la figura 5, se puede utilizar para generar un identificador de vitalidad y/o determinar la vitalidad del usuario. De manera más específica, el procesador de dispositivo móvil configurado, que emplea las etapas del proceso 500, puede extraer y registrar información dinámica de las características biométricas de Vitruvio y codificar las características como un identificador biométrico que indica vitalidad, y/o como un identificador exclusivo de vitalidad. Además, se debe comprender que el procesador configurado puede analizar la información dinámica para identificar el movimiento fluido de las características dentro de la secuencia de imágenes que son indicativas de vitalidad. Más concretamente, la vitalidad se puede determinar a partir del análisis del movimiento dinámico de las características de Vitruvio de bajo nivel para determinar si el flujo es representativo de un movimiento continuo. Del mismo modo, la vitalidad se puede determinar, asimismo, por el movimiento de las características de nivel intermedio, tal como los ojos, la boca y otras partes de la cara.

Además o alternativamente, el procesador configurado puede generar un identificador de vitalidad y/o determinar la vitalidad según los algoritmos de amplificación del movimiento de Euler, que también se conocen como amplificación de video de Euler (EMM o EVM). EMM se puede utilizar para amplificar pequeños movimientos del sujeto capturado en las imágenes, por ejemplo, enrojecimiento de la piel del sujeto durante un latido del corazón. En algunas implementaciones, cuando se emplea EMM, la cámara (por ejemplo, la cámara del teléfono inteligente) y el sujeto están quietos, no obstante, el procesador configurado puede utilizar EMM para detectar estos pequeños movimientos del sujeto incluso mientras el dispositivo se mueve, utilizando la estabilización de video.

En algunas implementaciones, se puede generar un identificador de vitalidad y/o determinar la vitalidad, analizando el movimiento de los labios, la dilatación de la pupila, el parpadeo y el movimiento de la cabeza a lo largo de la secuencia de imágenes. Además, también se puede generar un identificador de vitalidad y determinar la vitalidad analizando la grabación de audio de la voz del usuario, tal como comprenderían los expertos en la técnica. Además, en algunas implementaciones, la vitalidad también se puede determinar analizando los valores de luz asociados con características de nivel bajo, intermedio y/o alto representadas en una sola imagen y/o en múltiples fotogramas de imagen en la secuencia para determinar intensidades de luz anormales en el fotograma o fotogramas.

Además, la información basada en visión no artificial que incluye, el tiempo recibido de un reloj incorporado, la ubicación recibida de un dispositivo GPS, qué tan lejos de la cara del usuario se coloca la cámara durante la captura de imágenes, calculada a partir de las imágenes recibidas de la cámara u otro dispositivo de medición de distancia a bordo, la orientación del dispositivo móvil durante la adquisición de funciones, la aceleración del dispositivo móvil mientras el dispositivo móvil se coloca en posición para la adquisición tal como se recibe desde un acelerómetro se puede utilizar para generar un identificador que caracterice el comportamiento único del usuario características y/o analizados para determinar si la información es indicativa de vitalidad durante las sesiones de inscripción y autenticación.

Se debe comprender que uno o más identificadores de vitalidad generados de acuerdo con los métodos basados en imágenes y basados en visión no artificial pueden ser analizados y almacenados individualmente o combinados para generar uno o más identificadores biométricos y/o de vitalidad multidimensionales.

A continuación, en la etapa 355, se almacenan uno o más identificadores biométricos y uno o más identificadores de

vitalidad. En algunas implementaciones, el procesador del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de inscripción 176 y el módulo de base de datos 178, puede almacenar localmente los identificadores biométricos e identificadores de vitalidad, para llevar a cabo una autenticación mediante biometría en el dispositivo móvil 101a, evitando de este modo la transmisión de la información biométrica sensible al servidor del sistema para su almacenamiento.

En algunas implementaciones, el procesador del dispositivo móvil configurado puede transmitir los identificadores biométricos, los identificadores de vitalidad y otra información (por ejemplo, un ID de dispositivo móvil generado) al servidor 105 del sistema como uno o más paquetes de datos, por ejemplo, tal como se describe en la solicitud de patente de los Estados Unidos de Nº de serie 61/842.800, titulada “SYSTEM AND METHOD FOR PROVIDING BIOMETRICALLY AUTHENTICATED ACCESS USING MOBILE DEVICES”, presentada el 3 de julio de 2013, en tramitación con la presente y comúnmente asignada. Se debe comprender que se puede transmitir, asimismo, información adicional específica para un usuario y dispositivo móvil (por ejemplo, información de identificación de usuario) al servidor del sistema para asociar uno o más identificadores de vitalidad, identificadores biométricos e identificadores de dispositivo móvil con un usuario concreto.

Se debe comprender que algunas o todas las etapas del proceso de inscripción pueden ser repetidas utilizando otros dispositivos de usuario, por ejemplo, el dispositivo informático 101b de usuario. Por ejemplo, se puede generar un ID de dispositivo móvil exclusivo para otros dispositivos de usuario utilizados junto con el sistema 100, permitiendo de este modo la autorización del usuario utilizando múltiples dispositivos de usuario inscritos.

Pasando, a continuación, a la figura 4, que es un diagrama de flujo que ilustra una rutina 400 para autorizar a un usuario a acceder a un ACE de acuerdo con al menos una realización descrita en el presente documento.

El proceso comienza en la etapa 405, en la que se solicita al dispositivo móvil 101a que autentique al usuario 124. En algunas implementaciones, se solicita al dispositivo móvil que se autentique mediante la recepción de una entrada del usuario. Por ejemplo, el usuario puede iniciar la aplicación de cliente de autenticación segura que muestra un mensaje 630 en la pantalla táctil 600 del dispositivo móvil solicitando al usuario que introduzca la información de si desea autenticarse utilizando los botones virtuales 635, tal como se muestra en la figura 6B. En algunas implementaciones, el dispositivo móvil 101a puede comenzar el proceso de autenticación de manera automática. Por ejemplo, el dispositivo móvil puede solicitar al usuario que se autentique al detectar que el usuario ha utilizado el dispositivo móvil para acceder a un ACE que requiere autorización del usuario según lo especificado por la configuración del usuario o por la organización empresarial que opera el ACE.

En algunas implementaciones, el servidor 105 del sistema puede hacer que el dispositivo móvil 101a comience la autenticación en respuesta a la recepción de una solicitud de autorización. Preferiblemente, la solicitud de autorización incluye información de control de acceso que identifica al ACE. Además, la solicitud de autorización, preferiblemente, identifica al usuario 124 y/o a un dispositivo informático de usuario asociado, permitiendo de este modo que el servidor 105 del sistema haga que el dispositivo móvil del usuario apropiado comience la autenticación. De manera más específica, en respuesta a la solicitud de autorización, el servidor 105 del sistema puede realizar un cruce de referencias entre el usuario y/o dispositivo informático identificado en la solicitud con la base de datos de perfiles de usuario para determinar si el usuario o el dispositivo está asociado con un perfil de usuario y, por lo tanto, está inscrito en el sistema. Del mismo modo, el servidor del sistema puede determinar si el perfil del usuario identifica un dispositivo móvil inscrito, y transmitir una solicitud de autenticación biométrica al dispositivo móvil identificado, lo que hace que el dispositivo móvil autentique al usuario de manera biométrica.

A modo de ejemplo y sin limitación, el servidor del sistema puede recibir la solicitud de autorización directamente desde un dispositivo informático remoto 102 que controla el acceso al ACE (por ejemplo, un sistema informático de una institución financiera, un dispositivo informático en red que controla una cerradura electrónica de puerta que proporciona acceso a una ubicación restringida, un servidor web que requiere autenticación del usuario antes de permitir que el usuario acceda a un sitio web). A modo de ejemplo adicional, la solicitud de autenticación puede ser recibida por el servidor 105 del sistema desde un dispositivo informático del usuario (por ejemplo, el dispositivo informático 101b) que se está utilizando para obtener acceso a un entorno en red. En este ejemplo, el dispositivo informático 101b del usuario puede actuar como intermediario del servidor del lado del servidor del ACE transmitiendo la solicitud de autorización al servidor 105 del sistema, recibiendo respuestas del servidor del sistema y transmitiendo información al servidor del ACE para facilitar el acceso al ACE. Además o alternativamente, el servidor del sistema puede comunicarse directamente con los servidores del lado del servidor del ACE de acuerdo con las realizaciones dadas a conocer.

A continuación, en la etapa 410, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software, que incluyen el módulo de autenticación 180, el módulo de interfaz de usuario 170, el módulo de análisis 174 y el módulo de captura 172, captura la información biométrica actual del usuario. Además, el procesador configurado también puede capturar información actual basada en visión no artificial, así como información actual de identificación del dispositivo móvil. La captura de dicha información puede ser realizada por el dispositivo móvil de la manera descrita en relación con las etapas 315, 335 y 345 de la figura 3, y tal como se describe adicionalmente en el presente documento en relación con la figura 5.

A continuación, en la etapa 415, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software, que incluyen el módulo de autenticación 180 y el módulo de análisis 174, genera uno o más identificadores biométricos actuales de la manera descrita en relación con la etapa 340 de la figura 3, y tal como se describe adicionalmente en el presente documento en relación con la figura 5.

A continuación, en la etapa 420, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software, incluido el módulo de autenticación 180, el módulo de interfaz de usuario 170, el módulo de análisis 174, puede generar uno o más identificadores de vitalidad actuales utilizando la información biométrica actual y/o información actual no basada en visión artificial de la manera descrita en relación con las etapas 335 a 350 de la figura 3, y tal como se describe adicionalmente en el presente documento en relación con la figura 5.

Además, en la etapa 425, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software, que incluyen el módulo de autenticación 180, el módulo de interfaz de usuario 170, el módulo de captura 172 y el módulo de análisis 174, puede extraer la información de identificación del dispositivo móvil que está actualmente asociada con el dispositivo móvil 101a, y generar un identificador móvil actual sustancialmente de la misma manera que se describe en relación con las etapas 315 y 325 de la figura 3. Se debe comprender que dicha información y un identificador de dispositivo móvil no necesitan ser generados con cada sesión de autenticación. En algunas implementaciones, un identificador generado previamente, por ejemplo, el ID del dispositivo móvil generado durante la inscripción inicial, puede ser utilizado para identificar el dispositivo móvil.

A continuación, en la etapa 430, el usuario se autentica de acuerdo con al menos una parte del uno o más identificadores biométricos actuales. Utilizando los identificadores biométricos actuales, la identidad del usuario puede ser autenticada comparando los identificadores biométricos con uno o más identificadores biométricos almacenados que fueron generados previamente durante el proceso de inscripción o en las sesiones de autenticación posteriores. Se debe comprender que la etapa de autenticación biométrica no se limita a la utilización de identificadores biométricos de Vitruvio a modo de ejemplo, y puede utilizar cualquier número de otros identificadores biométricos generados de acuerdo con diversas modalidades de identificación biométrica (por ejemplo, iris, cara, voz, huella digital y similares).

En algunas implementaciones, el procesador del dispositivo móvil, configurado ejecutando uno o más módulos de software 130, que incluye, preferiblemente, el módulo de autenticación, autentica al usuario 124 haciendo coincidir al menos una parte del uno o más identificadores biométricos actuales generados en la etapa 515 con la versión o versiones generadas previamente, y determinando si coinciden en un grado requerido. Por ejemplo, el procesador del dispositivo móvil configurado puede aplicar un algoritmo de comparación para comparar al menos una parte de los identificadores biométricos actuales con la versión o versiones almacenadas y determinar si coinciden en un grado prescrito. De manera más específica, en un algoritmo de coincidencia a modo de ejemplo, el proceso de encontrar correspondencias de fotograma a fotograma (por ejemplo, de identificador actual a identificador almacenado) se puede formular como la búsqueda del vecino más cercano de un conjunto de descriptores para cada elemento de otro conjunto. Dichos algoritmos pueden incluir, entre otros, el emparejador de fuerza bruta y el emparejador basado en Flann.

El comparador de fuerza bruta busca cada descriptor en el primer conjunto y el descriptor más cercano en el segundo conjunto mediante la comparación de cada descriptor (por ejemplo, búsqueda exhaustiva). El comparador basado en Flann utiliza el algoritmo de búsqueda de vecino más cercano aproximado para encontrar correspondencias. El resultado de la coincidencia de descriptores es una lista de correspondencias entre dos conjuntos de descriptores. El primer conjunto de descriptores se conoce, en general, como el conjunto de entrenamiento porque corresponde a un patrón de datos (por ejemplo, el uno o más identificadores biométricos almacenados). El segundo conjunto se denomina conjunto de consultas, ya que pertenece a la “imagen”, en el que se buscará el patrón (por ejemplo, los identificadores biométricos actuales). Cuantas más coincidencias correctas se encuentren (por ejemplo, más patrones existan para las correspondencias de “imágenes”) más posibilidades hay de que el patrón esté presente en la “imagen”. Para aumentar la velocidad de coincidencia, el procesador puede entrenar a un emparejador antes de, o llamando a la función de coincidencia. La etapa de entrenamiento se puede utilizar para optimizar el rendimiento del emparejador basado en Flann. Para ello, el procesador configurado puede construir árboles de índices para descriptores de entrenamiento. Y esto aumentará la velocidad de coincidencia para grandes conjuntos de datos. Para el emparejador de fuerza bruta, en general, puede almacenar los descriptores de entrenamiento en los campos internos.

Además, en la etapa 435, el usuario se autentica adicionalmente verificando la vitalidad del usuario. En algunas implementaciones, la vitalidad del usuario puede ser determinada comparando al menos una parte del uno o más identificadores de vitalidad actuales generados en la etapa 420 con las versiones generadas previamente, y determinando si coinciden en un grado requerido. Tal como se señaló anteriormente, la verificación de la vitalidad del usuario también puede incluir el análisis de la información biométrica y no de visión artificial capturada y/o del identificador o identificadores de vitalidad, para determinar si muestran características de un sujeto vivo con una certeza prescrita. En algunas implementaciones, el procesador 110 configurado puede analizar la información dinámica codificada en el identificador de vitalidad, para determinar si la información muestra un movimiento fluido de las características biométricas dentro de la secuencia de imágenes que son indicativas de un sujeto vivo. Más concretamente, la vitalidad se puede determinar a partir del análisis del movimiento dinámico de las características

de Vitruvio de bajo nivel para determinar si el flujo es representativo de un movimiento continuo. Del mismo modo, la vitalidad se puede determinar, asimismo, por el movimiento de las características de nivel intermedio, tal como los ojos, la boca y otras partes de la cara. De manera similar, la vitalidad se puede determinar comparando el movimiento de las características de nivel intermedio del usuario con una o más caracterizaciones biométricas del usuario, para determinar si corresponden. Por ejemplo, los movimientos de los labios del usuario se pueden comparar con la impresión de voz del usuario, para determinar si el movimiento de los labios corresponde a las palabras pronunciadas por el usuario durante el proceso de captura en la etapa 410.

Si la vitalidad se determina haciendo coincidir los identificadores de vitalidad según un algoritmo de coincidencia o analizando la información capturada en la etapa 410, o los identificadores de vitalidad generados en la etapa 420 para los indicadores de vitalidad, puede depender de las limitaciones ambientales, por ejemplo, de la iluminación. De manera más específica, si la información biométrica se captura en condiciones de poca luz, la vitalidad se puede determinar utilizando algoritmos de coincidencia. Alternativamente, si la información biométrica se captura en condiciones de iluminación adecuadas, la vitalidad se puede determinar analizando la información capturada y/o los identificadores generados que caracterizan la información biométrica.

Además, la información actual basada en visión no por ordenador recopilada en la etapa 410 también se puede analizar y comparar con los rasgos de comportamiento establecidos por el usuario, para determinar si coinciden en un grado prescrito. Por ejemplo, los patrones de comportamiento basados en el tiempo y la ubicación se pueden identificar a lo largo del tiempo y la posición actual en comparación con el patrón, para determinar si se muestran diferencias (por ejemplo, comportamiento anormal). A modo de ejemplo adicional, la “oscilación” o aceleración particular del dispositivo móvil durante múltiples procesos de autenticación se puede caracterizar como un rasgo de comportamiento, y la oscilación particular del dispositivo durante la sesión de autenticación actual puede ser comparada para identificar un comportamiento anormal. Del mismo modo, la orientación del dispositivo o la distancia de la cara del usuario también se pueden comparar. Se debe comprender que este análisis puede ser realizado para determinar la vitalidad, así como para autenticar la identidad del usuario en relación con la etapa 435. Los sistemas y métodos a modo de ejemplo para determinar la vitalidad se describen con más detalle en el presente documento y en la Solicitud de Patente de los Estados Unidos de Nº de serie 14/201.462, titulada “SYSTEMS AND METHODS FOR DETERMINING LIVENESS”, presentada el 7 de marzo de 2014, en tramitación con la presente y comúnmente asignada.

A continuación, en la etapa 440, el usuario es autorizado por el servidor 105 del sistema. La autorización puede incluir verificar que un usuario inscrito que haya sido autenticado de manera biométrica utilizando un dispositivo móvil inscrito está intentando acceder al ACE.

En algunas implementaciones, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de autenticación 180 y el módulo de comunicación 182, puede generar al menos una solicitud de transacción y transmitir la solicitud de transacción al servidor 105 del sistema. Por ejemplo y sin limitación, la solicitud de transacción puede incluir: información que identifica al usuario (por ejemplo, información de identificación de usuario o un identificador de usuario generado durante la autenticación o inscripción); información que identifica el dispositivo móvil (por ejemplo, identificación del dispositivo móvil o un identificador del dispositivo móvil generado durante la autenticación o inscripción); información que indica si el usuario ha sido autenticado de manera biométrica; e información sobre el ACE al que el usuario está intentando acceder.

En algunas implementaciones, la solicitud de transacción puede incluir una clave de SSL privada de dos direcciones generada durante el proceso de inscripción, y que establece una sesión de comunicación segura de SSL de dos direcciones entre el dispositivo móvil 101a y el servidor 105 del sistema. La clave puede incluir información que identifique al usuario y al dispositivo móvil, por ejemplo, un identificador de usuario y un identificador de dispositivo móvil. Además o alternativamente, la clave puede incluir información que se puede utilizar para identificar el par de dispositivos móviles de usuario. Se debe comprender que la solicitud de transacción y/o la información incluida en la solicitud o solicitudes de transacción puede ser transmitida como varias transmisiones separadas. De manera similar, el procesamiento de la solicitud tal como se describe adicionalmente en la etapa 445 puede ser llevado a cabo en cualquier número de etapas por el dispositivo móvil 101a, o el servidor 105 del sistema, o por el dispositivo informático remoto 102, o por una combinación de los anteriores.

En respuesta a la recepción de la solicitud de transacción, el servidor 105 del sistema, utilizando un procesador 210 que se configura ejecutando uno o más módulos de software 130, puede procesar la solicitud de transacción para autorizar al usuario a acceder al ACE. Por ejemplo, el servidor del sistema puede realizar un cruce de referencias entre el usuario identificado en la solicitud de transacción y una base de datos de perfiles de usuario para determinar si el usuario está asociado con un perfil de usuario y, por lo tanto, está inscrito en el sistema 100. Del mismo modo, el servidor del sistema puede determinar si el dispositivo móvil identificado por la solicitud también está asociado con el perfil del usuario. En algunas implementaciones, el usuario puede ser autorizado mediante la comparación de la clave recibida con una o más claves almacenadas en asociación con los perfiles de usuario respectivos para identificar una coincidencia, verificando de este modo que el usuario y/o dispositivo móvil identificado por la clave corresponde a un perfil de usuario almacenado en la base de datos.

Además, la etapa de autorizar al usuario también puede incluir la determinación, por el servidor del sistema, de si la solicitud de transacción indica que el usuario ha sido autenticado de manera biométrica. En algunas implementaciones, verificar la autenticación biométrica puede incluir determinar si la solicitud de transacción se ajusta a una configuración predeterminada. Por ejemplo, la solicitud de transacción puede ser generada por el dispositivo móvil solo después de una autenticación biométrica con éxito del usuario por parte del dispositivo móvil. En consecuencia, la recepción de la solicitud de transacción proporciona la confirmación de que el usuario ha sido autenticado de manera biométrica. A modo de ejemplo adicional, la solicitud de transacción puede ser generada para incluir la clave que se puede utilizar para identificar al usuario y/o al dispositivo móvil solo después de una autenticación biométrica con éxito. A modo de ejemplo adicional, la solicitud de transacción puede incluir indicadores adicionales, indicadores, información de sesión y similares, que indican que el usuario ha sido autenticado de manera biométrica y, asimismo, puede proporcionar una seguridad adicional a la autenticidad de la transmisión.

De manera similar, se debe comprender que todas las transmisiones hacia y desde los diversos dispositivos informáticos (por ejemplo, el dispositivo móvil 101a, el dispositivo informático 101b del usuario, el servidor 105 del sistema y el dispositivo informático remoto 102) pueden tener una marca de tiempo y ser sensibles al tiempo, y/o incluir información de la sesión de comunicación. De este modo, el proceso de autorización puede depender, asimismo, de que la autenticación tenga lugar dentro de una duración predefinida o “tiempo de vitalidad” desde la marca de tiempo de cada paquete de datos que se envía al servidor del sistema. En el caso de un asalto de tipo malformado o MITM (hombre en el medio), en el que se rediseñó un paquete, el tiempo de vitalidad proporciona una seguridad adicional, ya que sería difícil reconstruir un nuevo paquete con los datos correctos dentro del tiempo en el que la TTL está configurada.

La autorización también puede incluir la determinación, por el servidor 105 del sistema, de si el usuario tiene permiso para acceder al ACE y/o realizar una transacción (por ejemplo, acceder a un sitio web seguro o realizar una transacción financiera, o acceder a información almacenada, etc.). Preferiblemente, durante el proceso de autorización, el servidor 105 del sistema recibe información de control de acceso que identifica al ACE. Por ejemplo, en el escenario en el que el dispositivo móvil inicia de manera automática la autenticación al detectar que el usuario está intentando acceder a un ACE, la solicitud de transacción puede incluir la información de control de acceso que identifica al ACE. A modo de ejemplo adicional, si se recibe una solicitud de autorización del servidor del sistema desde un dispositivo informático remoto asociado con un ACE, la solicitud de autorización puede incluir la información de control de acceso. En base al ACE identificado en la información de control de acceso, el servidor 105 del sistema puede determinar si el perfil del usuario identifica una o más cuentas de transacción que pueden ser utilizadas para acceder al ACE.

En algunas implementaciones, la solicitud de transacción, la solicitud de autorización y/o la información de control de acceso recibida por el servidor 105 del sistema pueden incluir detalles de transacción que describen la naturaleza del acceso de usuario solicitado, y/o una transacción concreta a ser realizada entre el usuario y el ACE. En consecuencia, la autorización del usuario por parte del servidor 105 del sistema puede incluir, además, autorizar el acceso y/o autorizar la transacción concreta. De manera más específica, el servidor 105 del sistema puede consultar uno o más almacenes de datos definidos para recopilar cualquier regla de acceso (por ejemplo, permisos de acceso, funciones, configuraciones, etc.) asociados con una o más de las cuentas de transacción del usuario y que gobiernan el acceso utilizando una o más cuentas de transacción. Asimismo, el servidor del sistema también puede recopilar reglas de acceso que rigen el acceso al ACE. Según las reglas de acceso y los detalles de la transacción recopilados, el servidor del sistema puede determinar si el usuario está autorizado para acceder al ACE y/o llevar a cabo la transacción solicitada.

A continuación, en la etapa 445, se genera una notificación de autorización de acuerdo con si el usuario está autorizado para acceder al ACE en la etapa 440. En alguna implementación, el servidor 105 del sistema puede transmitir la notificación de autorización, directamente al ACE, de que el usuario está intentando acceder, o indirectamente, a través de uno o más dispositivos informáticos que utiliza el usuario para acceder al ACE (por ejemplo, un dispositivo móvil 101a o un dispositivo informático 101b del usuario). Por ejemplo, la notificación de autorización puede ser transmitida a un dispositivo informático remoto 102 que controla el acceso al ACE y, por lo tanto, requiere la autorización del usuario (por ejemplo, un dispositivo informático en red que controla una cerradura electrónica que proporciona acceso a una ubicación restringida, un servidor que requiere autorización del usuario antes de permitir que el usuario acceda a un sitio web privado o a un almacén de datos seguro, un terminal de cajero automático que requiere autorización antes de dispensar fondos). A modo de ejemplo adicional, la notificación de autorización puede ser transmitida al dispositivo móvil 101a o al dispositivo informático 101b del usuario con el que el usuario está intentando obtener acceso a un ACE utilizando una cuenta de transacción. En función de la notificación de autorización, cualquier dispositivo informático remoto que reciba la notificación de autorización puede conceder acceso al usuario y/o autorizarlo además a acceder al ACE y/o a procesar la transacción solicitada.

El contenido y la forma de la notificación de autorización pueden variar según la implementación concreta del sistema 100. Por ejemplo, en el caso de que el usuario intente acceder a un sitio web, la notificación puede simplemente identificar al usuario e indicar que el usuario ha sido autenticado de manera biométrica y la identidad del usuario ha sido autorizada / verificada. Además o alternativamente, la notificación puede incluir información sobre una o más cuentas de transacción, por ejemplo, la información de inicio de sesión y contraseña del usuario o una contraseña de una sola utilización. En otros casos, por ejemplo, cuando el usuario intenta completar una

transacción financiera, la notificación puede incluir los datos de pago del usuario, los detalles de la transacción y similares. En algunas implementaciones, la notificación de autorización puede incluir una clave fusionada, que es una contraseña de autorización única que está fusionada con uno o más identificadores biométricos, del usuario, del dispositivo móvil o de vitalidad, información de identificación del usuario y/o información de identificación del dispositivo móvil, y similares. En una implementación de este tipo, el dispositivo informático que recibe la notificación de autorización puede deshacer la contraseña de una sola utilización de acuerdo con los identificadores correspondientes previamente almacenados por el dispositivo informático remoto, y utilizar la información codificada para conceder acceso al usuario.

Pasando ahora a la figura 5, un diagrama de flujo ilustra una rutina 500 para detectar las características biométricas del usuario a partir de una serie de imágenes de acuerdo con al menos una realización dada a conocer en el presente documento, y generar un identificador biométrico, con el fin de autenticar a un usuario y/o determinar la vitalidad del usuario. En general, la rutina incluye capturar y analizar una o más imágenes, preferiblemente una secuencia de imágenes, de al menos los ojos del usuario, la región periocular y la región facial circundante (conjuntamente, la región facial o la región de Vitruvio); identificar características espaciotemporales de bajo nivel de al menos los ojos y las regiones perioculares, con el fin de generar un identificador que comprima las características espaciotemporales de bajo nivel (el identificador biométrico de Vitruvio). En comparación con las características de alto nivel, que, en general, caracterizan el fotograma global de la imagen (por ejemplo, la imagen completa de la región facial del usuario), o características intermedias, que caracterizan los objetos dentro de los fotogramas de imagen más grandes (por ejemplo, la nariz), las características de bajo nivel se utilizan con frecuencia para representar características de la imagen y, en este caso, características biométricas. Las características de bajo nivel son preferibles, porque son robustas, para la caracterización de la imagen, ya que proporcionan invariancia bajo rotación, tamaño, iluminación, escala y similares.

La inclusión de la región periocular en la generación de un identificador biométrico puede ser beneficiosa ya que en las imágenes en las que las características del iris por sí solas no pueden ser obtenidas (o utilizadas) de manera fiable, la región de la piel circundante puede ser utilizada para caracterizar las características biométricas del usuario que pueden ser utilizadas para confirmar o refutar de manera efectiva una identidad. Además, la utilización de la región periocular representa un equilibrio entre utilizar toda la región de la cara y utilizar solo el iris para el reconocimiento. Cuando se obtiene una imagen de la cara completa desde una distancia, la información del iris es, habitualmente, de baja resolución, y la extracción de las características biométricas solamente de la modalidad de iris será deficiente.

Además, la agregación colectiva de características perioculares de bajo nivel genera de manera efectiva un identificador de Vitruvio que caracteriza las características de nivel superior, por ejemplo, características de nivel intermedio. La región periocular se puede considerar como una característica de nivel intermedio con un alto rendimiento en lo que respecta a la clasificación del sujeto, porque, en general, la región periocular proporciona una alta concentración de características exclusivas a partir de las que un usuario puede ser clasificado (de manera biométrica).

Se debe comprender que, de acuerdo con las realizaciones dadas a conocer, las imágenes pueden ser capturadas y el identificador biométrico que es indicativo de la identidad y/o vitalidad del usuario puede ser generado utilizando dispositivos móviles (por ejemplo, teléfonos inteligentes), que están disponibles de manera extendida y que tienen cámaras digitales capaces de capturar imágenes de la región de Vitruvio en las bandas espectrales visibles. No obstante, se debe comprender que los sistemas y métodos descritos pueden ser implementados utilizando dispositivos informáticos equipados con dispositivos de obtención de imágenes multiespectrales, que pueden obtener imágenes tanto en las bandas espectrales visibles como en las del IR cercano. Dichos dispositivos de usuario de obtención de imágenes multiespectrales pueden facilitar la captura de la textura del iris y la textura periocular.

El proceso comienza en la etapa 505, en la que el procesador 110 del dispositivo móvil configurado ejecutando uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172, hace que la cámara 145 capture una secuencia de imágenes de al menos una parte región de Vitruvio del usuario (124), y almacena la secuencia de imágenes en la memoria. La captura de la secuencia de imágenes incluye la detección, mediante la cámara 145 del dispositivo móvil, de la luz reflejada en una parte de la región de Vitruvio del usuario. Preferiblemente, la porción de la región de Vitruvio del usuario incluye un iris / los iris del usuario, un ojo o los ojos, la región periocular, la cara, o una combinación de lo anterior. Además, el procesador configurado puede hacer que el dispositivo móvil emita luz, al menos en el espectro visible, para mejorar la intensidad de la reflexión capturada por la cámara. Además, aunque no es necesario, el dispositivo móvil también se puede configurar para emitir luz infrarroja, con el fin de aumentar el espectro de la luz reflejada que es capturada por la cámara. Se debe comprender que la secuencia de imágenes incluye una pluralidad de fotogramas de imágenes que son capturados secuencialmente durante un período de tiempo.

A continuación, en la etapa 510, se analiza un primer fotograma de imagen y se identifican características de bajo nivel, y se registran sus posiciones relativas. De manera más específica, el procesador 110 del dispositivo móvil configurado mediante la ejecución de los módulos de software 130, que incluyen, preferiblemente, el módulo de análisis 172, analiza un primer fotograma de imagen individual para extraer / detectar información espacial de las

características biométricas de Vitruvio de bajo nivel que incluyen, preferiblemente, características perioculares. El procesador configurado puede detectar las características o “puntos clave” mediante la ejecución de un algoritmo de detección de puntos clave que incluye, entre otros, SIFT, SURF, FREAK, características binarias, Densa SIFT, ORB u otros algoritmos, ya sean conocidos en la técnica o nuevos. El procesador configurado codifica cada uno de los puntos clave detectados utilizando los valores de píxel (por ejemplo, el brillo y el color del píxel) que corresponden al punto clave identificado, definiendo de este modo un descriptor de clave local. Estas características de bajo nivel varían, en general, entre 3 píxeles y aproximadamente 100 píxeles de tamaño; no obstante, se debe comprender que las características de bajo nivel no están limitadas a encontrarse dentro del rango mencionado anteriormente. De manera similar a la mayoría de los descriptores de algoritmos de imagen (SIFT, SURF, FREAK, etc.), el conjunto de píxeles no representa necesariamente un área cuadrada. El cálculo de cada característica implica estimaciones de histograma exhaustivas que se toman, por ejemplo, en más de 16x16 regiones. Se debe comprender que se puede considerar que el tamaño del histograma o región representa la fuerza de la característica y es una función no lineal de los píxeles (por ejemplo, no es necesariamente una función de la calidad de la imagen).

A continuación, en la etapa 515, se analiza una serie continua de fotogramas posteriores y se extrae información espacial y/o dinámica de los puntos clave identificados en la etapa 510. Utilizando los descriptores de los puntos clave codificados / generados en la etapa 510, el procesador 110 del dispositivo móvil, que se configura ejecutando los módulos de software 130, que incluyen, preferiblemente, el módulo de análisis 172, analiza una pluralidad de fotogramas posteriores para identificar los puntos clave correspondientes en cada una las imágenes posteriores en la secuencia de imágenes. De manera más específica, los píxeles que definen los descriptores de puntos clave locales son detectados en los fotogramas de imagen posteriores, y se extrae información espacial y dinámica para los píxeles detectados. Dicha información dinámica incluye el movimiento relativo de los píxeles a lo largo de la serie de fotogramas de imágenes de píxeles. Por ejemplo, el procesador configurado puede analizar los siguientes, por ejemplo, 5 a 10 fotogramas en la secuencia de la imagen mediante la aplicación de un algoritmo (por ejemplo, los algoritmos de Lukas Kanade o Brox y similares) para detectar los píxeles correspondientes a los puntos clave en cada una de las imágenes en la secuencia. El procesador configurado puede realizar un seguimiento de la posición de un conjunto de píxeles de muestra, disperso o denso, a través de los fotogramas, y registrar las posiciones.

La posición relativa (por ejemplo, movimiento) de un píxel de un fotograma de imagen a otro se denomina “desplazamiento de flujo óptico” o “flujo”. Se debe comprender que el desplazamiento del flujo óptico también se puede muestrear utilizando otros métodos de análisis recursivo de múltiples fotogramas.

El procesador configurado puede cuantificar la cantidad total de puntos llenándolos espacial y temporalmente en contenedores de histograma que pueden codificarse en la memoria del dispositivo móvil. En el que cada contenedor representa cuánto 'flujo óptico' y 'gradientes' espaciales existen en los grupos de píxeles asociados con un descriptor de punto clave concreto.

Preferiblemente, el procesador configurado puede llenar los histogramas, de acuerdo con algoritmos, que incluyen, pero no están limitados a, HOOF, HOG o SIFT y similares. En consecuencia, las rutas se pueden definir como histogramas de gradientes orientados (temporales o espaciales) e histogramas de flujos orientados.

Los gradientes temporales representan el cambio de posición en el tiempo (dirección, magnitud, tiempo entre los fotogramas de la imagen), por ejemplo, el flujo de un píxel o píxeles. Por ejemplo, una intensidad de píxel identificada en el primer fotograma de imagen que, a continuación, es identificado en otra ubicación de píxel en un segundo fotograma de imagen en la secuencia, se puede expresar como un gradiente temporal. Los gradientes espaciales representan la diferencia de intensidades alrededor de un píxel o grupos de píxeles concretos, en un fotograma de imagen. Por ejemplo, la intensidad de un píxel X en un primer fotograma de imagen y la intensidad de los píxeles circundantes X-1, X+1, Y-1, Y+1, se pueden representar como un gradiente orientado que muestra la diferencia de intensidad entre X y los píxeles circundantes X-1, X+1, etc. A modo de ejemplo adicional, un píxel negro justo al lado de un píxel blanco que está justo al lado de un píxel negro es un gradiente muy fuerte, mientras que tres píxeles blancos seguidos no tienen gradiente.

En consecuencia, tanto la información espacial como la temporal se definen en los histogramas. El acoplamiento de dicha información espacial e información temporal permite que una única caracterización de Vitruvio sea tanto una función del contenido de una sola imagen como del contenido del movimiento dinámico a lo largo del tiempo a través de múltiples imágenes.

Se debe comprender que se pueden llevar a cabo una o más operaciones de procesamiento previo en los fotogramas de imagen antes de llevar a cabo las etapas 510 y 515. Por ejemplo y sin limitaciones, el procesamiento previo de los datos de la imagen antes del análisis puede incluir escalar, orientar los fotogramas de la imagen en el espacio de coordenadas y similares, como comprenderían los expertos en la técnica.

Asimismo, se debe comprender que el procesador configurado puede llevar a cabo operaciones adicionales de procesamiento previo en la información espacial y temporal, antes de completar la información en los histogramas. Por ejemplo y sin limitación, el procesamiento previo puede incluir calcular combinaciones algebraicas de las derivadas de las rutas de flujo rastreadas, texturas derivadas espaciales más profundas, texturas de las derivadas espaciales, histogramas de límites de movimiento similares a Inria CVPR 2011, Kalman, filtros, algoritmos de

estabilización y similares.

A continuación, en la etapa 520, se identifican las continuidades de los píxeles sobresalientes. El procesador 110 del dispositivo móvil, que se configura ejecutando los módulos de software 130, que incluyen, preferiblemente, el módulo de análisis 172, puede identificar continuidades de píxeles sobresalientes analizando el "flujo óptico" de los píxeles a lo largo de la secuencia de fotogramas y grabados en los histogramas.

En general, la ruta de movimiento de uno o más píxeles puede ser analizada y comparada con los criterios prescritos para determinar qué característica muestra el flujo (por ejemplo, es el flujo representativo de un píxel estático, una posición continuamente cambiante, de movimiento no fluido, tal como saltar alrededor del fotograma de la imagen, etc.). Preferiblemente, las continuidades de píxeles más destacadas son aquellos píxeles y grupos de píxeles que tienen valores de flujo óptico que son continuos.

De manera más específica, el procesador configurado puede comparar los gradientes de flujo óptico de un píxel con un conjunto prescrito de criterios de continuidad que se definen para garantizar la presencia de dinámica de flujo. Por ejemplo y sin limitación, los criterios de continuidad pueden incluir, pero no están limitados a, la presencia de derivadas más profundas en las pistas de flujo del píxel que define un punto clave concreto. A modo de ejemplo adicional, se pueden establecer criterios de continuidad mediante el análisis de secuencias de imágenes capturadas de sujetos vivos para identificar valores / características de flujo óptico mostradas por sujetos vivos en comparación con valores / características de flujo mostrados por imágenes tomadas de sujetos no vivos. Se debe comprender que estas características pueden ser exclusivas para el usuario o pueden ser características compartidas por otros sujetos vivos. Si el píxel asociado con un punto clave concreto tiene un flujo que cumple con los criterios de continuidad, el píxel concreto puede ser identificado como continuidades sobresalientes. En otras palabras, si el píxel muestra un flujo que cumple con los criterios de continuidad, el píxel o grupo de píxeles puede ser determinado para indicar vitalidad. Si se encuentran píxeles que muestran la vitalidad, entonces el procesador puede determinar que el sujeto de las imágenes está vivo, determinando, por lo tanto, la vitalidad, tal como se describe más adelante en el presente documento.

Se debe comprender que, debido a que los contenedores de histograma son esencialmente distribuciones de áreas de píxeles, el procesador configurado puede analizar el flujo píxel a píxel, o grupos mayores de píxeles asociados (por ejemplo, múltiples píxeles que definen un punto clave concreto).

A continuación, en la etapa 525, las primitivas de Vitruvio se pueden calcular basándose, entre otras cosas, en las continuidades de píxeles sobresalientes identificadas en la etapa 520. Las primitivas de Vitruvio son construcciones informáticas que caracterizan la región de Vitruvio de un usuario concreto de acuerdo con la disposición espacial de las características identificadas en la etapa 510 y con la información dinámica identificada en 515. De manera más específica, las primitivas se calculan, utilizando el procesador de dispositivo móvil configurado, en el espacio de las distribuciones de histograma. Debido a que el espacio de los histogramas puede ser muy costoso desde el punto de vista informático, y que los dispositivos móviles, en general, no son tan potentes desde el punto de vista informático como los sistemas tradicionales de autenticación biométrica, las primitivas de Vitruvio se pueden calcular en el espacio de los histogramas, lo que da como resultado histogramas con menor complejidad informática.

En algunas implementaciones, el procesador configurado puede expandir la agrupación de puntos clave espaciales a combinaciones algebraicas más altas de formas de gradiente, lo que resulta en todas las distribuciones espaciotemporales posibles de cantidades agrupadas. El procesador configurado puede calcular las características en un dominio espaciotemporal corto, por ejemplo, fotogramas de imagen de hasta 5 píxeles. Sin embargo, se debe comprender que se puede utilizar un dominio espaciotemporal más corto o más largo. Por ejemplo, cuando se aplica el acoplamiento euleriano, es preferible un dominio más largo.

A continuación, en la etapa 530, el procesador configurado almacena las primitivas de Vitruvio en la memoria del dispositivo móvil como un identificador de Vitruvio. Además, el procesador configurado puede generar y almacenar uno o más identificadores biométricos que incluyen al menos el identificador de Vitruvio.

Se debe comprender que, si bien la rutina 500 se describe en referencia a la generación de un identificador de Vitruvio, dichos términos no deben ser interpretados como limitativos, ya que la rutina 500 es aplicable a la extracción y caracterización de cualquier número de características biométricas a partir de imágenes de cualquier parte o partes del cuerpo de un individuo, que incluye, entre otros, la cara del usuario, los ojos (incluido el iris) y/o la región periocular, para definir un identificador biométrico. Además, la rutina 500 también es aplicable a la identificación y caracterización de características de imágenes de sujetos no humanos.

También se puede apreciar que, además de caracterizar a un usuario generando un identificador de Vitruvio de acuerdo con la rutina 500, tal como se ha descrito anteriormente, se pueden extraer características biométricas adicionales de la secuencia de imágenes capturadas en la etapa 505, o capturadas por separado de la etapa 505. Dichas características biométricas adicionales pueden incluir, a modo de ejemplo y sin limitación, rasgos biométricos blandos. Los rasgos "biométricos blandos" son características humanas físicas, conductuales o adheridas en comparación con los datos biométricos duro, tal como huellas dactilares, iris, características perioculares y similares, que en general, son invariables. Sin embargo, se debe comprender que ciertas características dentro de la región

periocular pueden ofrecer información sobre características que se pueden utilizar como los datos biométricos blandos, tal como la forma de los ojos. A modo de ejemplo adicional, los rasgos biométricos blandos pueden incluir rasgos físicos tales como texturas de piel o colores de piel. Los datos biométricos blandos pueden incluir, asimismo, el movimiento detectado por el giroscopio / acelerómetro de un teléfono inteligente, las características del movimiento ocular detectadas por los algoritmos de seguimiento ocular y las características del movimiento de la cabeza detectadas mediante el seguimiento del movimiento de una cara y/o cabeza.

Dichos rasgos biométricos se pueden extraer y caracterizar de acuerdo con el método anterior, así como con los algoritmos de análisis biométrico existentes. Además, las caracterizaciones adicionales de las características biométricas del usuario pueden ser codificadas como parte del identificador de Vitruvio simultáneamente a la ejecución de la rutina a modo de ejemplo 500, o ser incluidas de otro modo en un identificador biométrico que incluya el identificador de Vitruvio, por ejemplo, fusionando los identificadores biométricos blandos con el identificador de Vitruvio.

También se debe comprender que el identificador biométrico no se limita a incluir el identificador de Vitruvio a modo de ejemplo y puede incluir cualquier número de representaciones biométricas alternativas de un usuario, tal como identificadores generados de acuerdo con las modalidades de identificación biométrica conocidas (por ejemplo, iris, cara, voz, huella digital y similares).

Según otro aspecto destacado de la solicitud del asunto, el identificador biométrico que se genera, entre otras cosas, extrayendo información dinámica mediante la selección de continuidades de píxeles sobresalientes y registrando los gradientes temporales, por ejemplo, 'flujo', caracteriza las características biométricas del usuario, y también es indicativo de la vitalidad del usuario. En consecuencia, además de generar un identificador de Vitruvio que también es indicativo de la vitalidad, el proceso 500 también puede ser implementado para determinar la vitalidad y/o generar un identificador de vitalidad con el propósito de determinar la vitalidad del usuario. De este modo, el procesador del dispositivo móvil configurado que emplea una o más de las etapas del proceso 500, puede extraer y registrar información dinámica de puntos clave locales en las imágenes, y analizar la información dinámica para, como mínimo, identificar continuidades sobresalientes que muestran flujo para definir un identificador de vitalidad. Se debe comprender que el identificador de vitalidad puede ser separado o incorporado, de manera integral, al identificador de Vitruvio generado mediante el proceso 500 a modo de ejemplo. De este modo, las referencias al identificador de vitalidad pueden ser interpretadas como un identificador distinto o como el identificador de Vitruvio.

Además, tal como se explicó anteriormente en relación con las figuras 3 a 5 y se explica más adelante en el presente documento, la vitalidad se puede determinar diferenciando entre una cara real y un intento de suplantación de identidad en el proceso de autenticación utilizando, por ejemplo, una fotografía o video de una cara.

Algunos sistemas de detección de vitalidad intentan distinguir entre rostros reales y fotografías y videos “para falsificación de identidad' mediante el análisis de la calidad de la imagen del rostro. Por ejemplo, las fotografías y los videos pueden tener una relación de contraste más baja que la de una cara real, o pueden tener una resolución más baja y, por lo tanto, parecen menos nítidos. Sin embargo, puede ser difícil para una cámara identificar dichas diferencias si la impresión de la falsificación de imagen también es de alta calidad de imagen. Otros sistemas de detección de vitalidad comprueban que la cara está viva solicitando al usuario que realice acciones a petición, por ejemplo, pidiéndole que parpadee en un momento determinado. Un inconveniente de esta técnica es que las acciones del usuario deben ser interrumpidas para pasar la prueba. De este modo, los sistemas de detección de vitalidad que pueden operar de manera fiable sin requerir acciones del usuario pueden ser beneficiosos.

De acuerdo con las realizaciones dadas a conocer, la vitalidad se puede determinar en base a una o más características de reflectividad de las imágenes capturadas por la cámara del dispositivo móvil, por ejemplo, iluminando la cara utilizando luz del visualizador o un emisor de luz, y determinando que las características de reflectividad de una o más imágenes capturadas por la cámara son compatibles con las de una cara real, y/o que las características de reflectividad de la imagen de la cámara no son compatibles con las de una fotografía o visualizador de video u otro objeto.

Pasando ahora a la figura 7, un diagrama de flujo ilustra una rutina 700 para detectar la vitalidad del usuario a partir de una o más imágenes de acuerdo con al menos una realización dada a conocer en el presente documento utilizando, por ejemplo, un dispositivo móvil 101a que tiene un procesador 110 que está conectado operativamente a uno o más emisores de luz. En algunas implementaciones, los emisores de luz pueden ser diodos emisores de luz (LED - Light Emitting Diodes, en inglés) que pueden emitir luz en el espectro visible, en el espectro infrarrojo (IR), en el espectro de IR cercano (NIR - Near InfraRed, en inglés) y similares, o cualquier combinación de los anteriores. Los sistemas y métodos para determinar la vitalidad en función de las características de reflectividad de las imágenes de los rasgos faciales (por ejemplo, de los ojos, la piel, la córnea y similares) se describen con más detalle en el presente documento y en la solicitud de patente de los Estados Unidos de Nº de serie 14/201.462, titulada “SYSTEMS AND METHODS FOR DETERMINING LIVENESS”, presentada el 7 de marzo de 2014, en tramitación con la presente y comúnmente asignada.

Para distinguir de manera más fiable el ojo real de un usuario de un impostor, por ejemplo, una impresión de alta resolución del ojo del usuario (por ejemplo, 'suplantación de identidad'), el procesador del dispositivo móvil puede

capturar imágenes de los ojos / cara del usuario y analizar las imágenes para garantizar que las características de reflexión concretas de una córnea humana están presentes en la imagen capturada. En algunas implementaciones, esto se puede realizar pulsando la intensidad de uno o más de los LED, y capturando imágenes mientras pulsa los LED utilizando la cámara (etapa 710). En el caso de una reflexión de córnea impresa, la reflexión estará presente continuamente en las imágenes capturadas, en el caso de la córnea genuina, los reflejos representados en las imágenes parpadearán como lo hace el LED. En consecuencia, al analizar los reflejos, el procesador del dispositivo móvil puede distinguir entre los reflejos del LED de una córnea genuina y una impresión que incluye una imagen de un reflejo en la córnea.

En una realización preferida, uno de los LED permanece encendido continuamente y uno de los LED NIR se pulsa a 3 Hz con una intensidad que varía sinusoidalmente; y la cámara tiene una velocidad de fotograma de más de 12 fotogramas por segundo (fps). Preferiblemente, la cámara captura múltiples fotogramas de imagen para análisis, por ejemplo, 30 imágenes. A continuación, el procesador puede analizar las imágenes capturadas y seleccionar, una o más imágenes que tengan la más alta calidad de imagen (por ejemplo, brillante y sin borrosidad) para ser utilizadas para el reconocimiento del patrón del iris para identificar al usuario (etapa 715). Todas las imágenes, o un subconjunto, se pueden utilizar para detectar la presencia de reflejos de la córnea y determinar la vitalidad, tal como se describe más adelante en el presente documento.

Para detectar reflejos, el procesador puede alinear las imágenes para que todas las imágenes del iris se produzcan en la misma posición en cada imagen (etapa 720). Se puede apreciar que las imágenes alineadas proporcionan datos relacionados con la intensidad del iris espacialmente (tal como una fotografía) y temporal (tal como un video).

A continuación, en la etapa 725, para cada píxel espacialmente, el procesador puede procesar los datos de intensidad temporal para determinar la magnitud del componente de frecuencia a 3 Hz, y dividir esto por la magnitud del componente de frecuencia a 0 Hz. Por ejemplo, esto puede ser llevado a cabo por el procesador utilizando un filtro Goertzel. Como resultado, el procesador puede generar una imagen que muestra la intensidad del reflejo del LED pulsante en comparación con la intensidad del reflejo del LED continuo (etapa 730). Tal como pueden comprender los expertos en la técnica, la composición física de un ojo / córnea genuina no refleja la misma cantidad de luz que una reproducción no genuina, ni refleja la luz exactamente de la misma manera. En consecuencia, el procesador puede analizar la imagen resultante para determinar si las intensidades de reflexión son indicativas de una córnea genuina o de una córnea reproducida (etapa 735). En el caso de la imagen de un ojo impreso, la imagen resultante puede tener una intensidad, en general, constante, y una intensidad de aproximadamente el 50 % de una córnea genuina. En el caso de una córnea genuina (por ejemplo, capturada de un sujeto vivo), la imagen resultante debe mostrar un pico agudo de alta intensidad correspondiente a la reflexión que solo es creado por el LED pulsante, y no por el LED continuo. Además, el procesador también puede detectar diferencias de intensidad debido a las sombras creadas en la región periocular, lo que da una indicación adicional de que la imagen obtenida tiene un perfil 3D y, por lo tanto, es un sujeto vivo.

Además, en la etapa 740, el procesador puede analizar la imagen resultante utilizando un algoritmo de procesamiento de imagen, para verificar que la imagen resultante sea compatible con la esperada de una región periocular genuina. Se puede apreciar que el reflejo de la luz de una córnea genuina es una función de la curvatura del ojo, que varía con respecto al reflejo de una reproducción, por ejemplo, una imagen plana de la córnea. Como resultado, el patrón de luz reflejada (por ejemplo, la concentración) varía en consecuencia. En algunas implementaciones, la imagen se puede comparar con una o más imágenes, generadas de manera similar, de regiones perioculares genuinas (por ejemplo, del usuario o de otros usuarios) o se puede comparar con características prescritas identificadas mediante el análisis de imágenes de regiones perioculares genuinas. Por ejemplo, el procesador puede emplear un clasificador de pelo y/o algoritmo para detectar la presencia de un pico de reflexión fuerte dentro de la región de la pupila, y de un tamaño / concentración esperada de la reflexión.

A continuación, en la etapa 745, el procesador puede calcular un nivel de confianza que indica la probabilidad de que las imágenes sean capturadas de una región periocular genuina. Por ejemplo, el nivel de confianza puede ser una función de lo estrechamente que la imagen resultante coincide con una o más imágenes generadas previamente o con características prescritas (por ejemplo, tal como se determina en la etapa 740). Además, el nivel de confianza puede ser una función de si la intensidad muestra una intensidad más constante característica de la imagen de una región periocular no genuina, o muestra picos agudos de alta intensidad correspondientes a la reflexión, que son características de la imagen de una región periocular genuina (por ejemplo, tal como se determinó en la etapa 735). Si el nivel de confianza de vitalidad supera un umbral de nivel de confianza prescrito, el procesador puede determinar que el usuario está vivo y autenticar al usuario en consecuencia.

En otras realizaciones, los LED se pueden pulsar fuera de fase entre sí. Las frecuencias del LED pulsante y el número de capturas de fotogramas pueden ser ajustados. La luz pulsante permite que el sistema reduzca la velocidad de captura de fotogramas para obtener imágenes más detalladas. Por ejemplo, pulsar los LED fuera de fase o en diferentes frecuencias puede permitir que el sistema capture datos para determinar la vitalidad en diferentes espectros. Además, los LED pulsantes a diferentes frecuencias se pueden utilizar para realizar análisis en diferentes escenarios de luz ambiental. Por ejemplo, en exteriores, donde los niveles de luz IR ambiental son altos, y en interiores, donde los niveles de IR son más bajos. También se pueden emitir ráfagas de luz IR que pueden mejorar la calidad de los datos recopilados en comparación con un solo flujo de luz y pueden prolongar la vida útil

del LED. La frecuencia de pulsación también se puede variar para evitar desencadenar respuestas físicas adversas de los usuarios, por ejemplo, reacciones epilépticas. Además, la simple sustracción de imágenes podría ser utilizada en lugar del análisis de frecuencia de pulso para reducir el número de fotogramas requeridos.

Además o alternativamente, el procesador 110 del dispositivo móvil, que ejecuta uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172, y el módulo de análisis 174, puede capturar imágenes del usuario utilizando la cámara del dispositivo móvil, y puede analizar las imágenes para detectar la presencia de la cara del usuario, por ejemplo, mediante la utilización de reconocimiento de forma u otras técnicas conocidas de identificación de caras. Una vez que se detecta la cara en las imágenes, el procesador configurado puede localizar de manera similar uno o más de los ojos del usuario en las imágenes. Además, el procesador 110 del dispositivo móvil configurado puede hacer que el visualizador (o un emisor de luz) sea pulsado, por ejemplo, cambiando la intensidad de la luz emitida por el visualizador. Preferiblemente, la intensidad es pulsada con el tiempo de manera sinusoidal a una frecuencia de 3 Hz, durante 2 segundos. Durante este tiempo, el procesador configurado, utilizando la cámara, puede capturar imágenes del ojo y grabar las imágenes, preferiblemente, a una velocidad de fotograma de al menos el doble de la frecuencia de la pulsación del visualizador (por ejemplo, un flash).

En una realización adicional, a medida que se graban las imágenes, se puede rastrear la posición del ojo para que todas las imágenes a analizar sean del ojo y tengan al menos una alineación, en general, compatible entre las mismas. Se puede apreciar que el seguimiento ocular se puede llevar a cabo de acuerdo con las realizaciones dadas a conocer y/o la posición ocular conocida o los algoritmos de seguimiento ocular, tal como comprenderían los expertos en la técnica. En algunas implementaciones, el procesador configurado puede hacer que se muestre un logotipo animado o información, tal como una fuente de noticias, durante la medición para atraer los ojos del usuario a una posición particular y entretener al usuario durante el proceso de captura de imágenes.

Después de la recopilación de imágenes, el procesador 110 del dispositivo móvil, que se configura ejecutando uno o más módulos de software 130, incluido el módulo de análisis 174, puede llevar a cabo un análisis de las imágenes para verificar que las características de reflectividad del ojo sean compatibles con las de un ojo verdadero, y no una fotografía. En algunas implementaciones, el procesador configurado puede analizar las características de reflectividad para determinar si la superficie curva de la córnea ha producido un reflejo pequeño, nítido y especular del visualizador que es visible para la cámara, tal como se explicó anteriormente. Una fotografía / video, en general, produce una reflexión difusa que es uniforme en toda la imagen, o una reflexión especular desde una superficie plana, que la hace mucho más grande que la de un ojo.

Además, cada píxel de la secuencia de fotogramas puede ser analizado, por el procesador 110 configurado, para identificar la fuerza del componente de frecuencia en la frecuencia de pulsación del visualizador (conocida como la “señal de potencia”). Por lo tanto, se puede crear una imagen de 'imagen de potencia' en la que la intensidad de cada píxel es la señal de potencia.

Una imagen de potencia de un ojo real contendrá un pico sobre la córnea del ojo. El procesador 110 configurado comprueba la presencia de un pico, por ejemplo, aplicando un filtro de paso de banda sobre la imagen para eliminar el ruido de alta frecuencia y el fondo de baja frecuencia, a continuación, encuentra la señal de potencia máxima en la imagen de potencia y, luego, verifica que el pico es del tamaño y la magnitud esperados sobre el fondo. Se puede realizar una determinación de la vitalidad con estos datos.

Alternativamente, la señal de potencia puede ser calculada como una relación de la intensidad de la señal a la frecuencia de pulsación del visualizador dividida por la suma de la intensidad de la señal en otras frecuencias. Esto significa que si la señal es ruidosa (y existen otras frecuencias quizás debido al movimiento o al desenfoque del movimiento), la señal de potencia se reduce y, por lo tanto, se descuenta de la imagen de potencia final. Dicho ruido del movimiento puede estar presente durante, por ejemplo, el movimiento ocular, el movimiento fotográfico o el movimiento en una suplantación de identidad mediante un video.

Además, la fase de la señal de potencia en la frecuencia de pulsación del visualizador se puede calcular y comparar con la fase de la frecuencia de pulsación del visualizador. Si la fase de la señal de potencia no está en fase con la frecuencia de visualización, entonces el procesador 110 configurado puede concluir que la señal de potencia debe ser de ruido, y ser descontada o atenuada como un indicador de vitalidad.

En algunas implementaciones, para la velocidad de análisis, el procesador 110 configurado podría utilizar un filtro Goertzel para medir la señal de potencia a intervalos sobre el espectro de frecuencia.

Además o alternativamente, el dispositivo móvil se puede configurar para analizar las características de reflectividad de las imágenes capturadas por la cámara, tal como se explicó anteriormente, excepto por que el visualizador puede pulsar para la suma de dos (o más) frecuencias, por ejemplo 3 Hz y 2 Hz, con una diferencia de fase concreta, digamos 180 grados. En consecuencia, la señal de potencia se calcula como la suma de la señal a 2 Hz y a 3 Hz dividida por la señal a otras frecuencias.

La señal de fase se puede calcular como la diferencia entre la fase a 2 Hz y a 3 Hz, y cuanto más se desvía la fase de la señal de los 180 grados esperados, más se descuenta o atenúa como un indicador de vitalidad.

En algunas implementaciones, la imagen de potencia puede utilizar 'superpíxeles' para reducir el ruido de cuantificación. La cuantificación ocurre cuando la intensidad de cada píxel en los fotogramas de imagen de la cámara se almacena como un valor discreto (habitualmente un número entero de 0 a 255). Para reducir los efectos negativos de esta cuantificación en la señal de potencia, se puede promediar cada píxel con los píxeles circundantes (por ejemplo, utilizando un desenfoque gaussiano con un diámetro de desenfoque aproximadamente igual al ancho del tamaño esperado de la reflexión del visualizador desde el ojo) para crear un 'súper píxel' que tiene menos artefactos de cuantificación. Estos superpíxeles se almacenan con una mayor precisión de intensidad que en los fotogramas de imagen originales (tal como con un número de coma flotante de 32 bits o un entero de 16 bits que proporciona valores de intensidad con 65.536 pasos en lugar de 255). Esto aumenta la calidad de la señal de potencia que se puede derivar y hace que los sistemas sean menos propensos a errores.

En una realización adicional, el dispositivo móvil se puede configurar para pulsar el visualizador y analizar las características de reflectividad de las imágenes capturadas por la cámara, tal como se explicó anteriormente, excepto por que la fase de la pulsación del visualizador es diferente para cada canal de color. Esto tiene el resultado de hacer que el color del visualizador cambie con el tiempo, y la imagen de fase se puede calcular en función de la diferencia de fase esperada entre cada canal de color. Por ejemplo, al hacer que los canales rojo y azul tengan fase de 0 grados, y el canal verde tenga fase de 180 grados, el visualizador pulsará entre verde y magenta.

En otra realización, en lugar de, o además de detectar el pico de reflexión de la córnea, el procesador configurado que ejecuta el algoritmo de análisis verifica la presencia de sombras de la iluminación del visualizador en la cara, y comprueba que sean compatibles con las de una cara real y no una fotografía o video. Por ejemplo, esto se podría realizar utilizando un clasificador de Haar en la imagen de potencia, o una 'imagen de sombra', que es una combinación de la imagen de potencia y la imagen de potencia a 0 Hz.

A pesar de las realizaciones anteriores, a modo de ejemplo, para analizar las características de reflectividad de las imágenes capturadas por la cámara para determinar si la reflectividad es compatible con una córnea viva, se pueden llevar a cabo métodos similares para determinar que la reflectividad no es compatible con la reflectividad de una impresión o visualizador de video de alta resolución.

Una característica de casi todas las impresiones y visualizadores de video es que son sustancialmente planos. Por lo tanto, la reflexión especular desde su superficie será similar a la de un espejo plano. Cuando se presenta una impresión o video de una cara (mirando directamente) a la cámara del teléfono inteligente, la cámara del teléfono inteligente podría capturar un reflejo del visualizador del teléfono inteligente en la impresión o video causado por los reflejos especulares. Dicho reflejo no se espera de una persona viva, porque la piel humana tiene una reflectividad altamente difusa y la cara no es plana.

La reflexión del visualizador se podría detectar (por ejemplo) mediante la utilización de métodos similares a los utilizados para detectar las reflexiones del visualizador desde la córnea del ojo. Por ejemplo, el visualizador podría ser pulsado a una frecuencia conocida y el reflejo del visualizador podría aislarse del fondo aislando los cambios de intensidad a esa frecuencia. De manera similar, el visualizador podría mostrar un patrón de manera espacial, y la presencia de este patrón se podría buscar en la imagen de la cámara por el procesador 110 del dispositivo móvil, que se configura ejecutando los módulos de software 130, que incluyen, preferiblemente, el módulo de análisis 174.

El patrón de reflexión se puede comparar con patrones de reflexión conocidos y con las características de diversas superficies (por ejemplo, una fotografía o visualizador de video) y, si el reflejo del visualizador es compatible con el de una superficie sustancialmente plana, entonces el procesador configurado puede determinar que las imágenes son el resultado de un intento de suplantación de identidad. De manera similar, si el reflejo es compatible con una impresión o video que se ha curvado en una sola dimensión (u otras formas no similares a una cara), el procesador también puede determinar que las imágenes son el resultado de un intento de suplantación de identidad. De manera similar, si el reflejo es compatible con el de un visualizador con un recubrimiento antideslumbrante difusivo (tal como el utilizado en algunos paneles de visualizador de cristal líquido), las imágenes son el resultado de un intento de suplantación de identidad.

Además o alternativamente, el procesador 110 del dispositivo móvil configurado puede analizar las imágenes para verificar que el reflejo del visualizador en la cara es más fuerte que el del fondo. Para ello, el procesador 110 configurado puede promediar todas las intensidades de píxeles de la región de la cara y buscar la frecuencia del flash del visualizador, y comparar esto con la misma figura para los píxeles del fondo. Se puede esperar que el reflejo de la cara sea más fuerte que el fondo porque está más cerca del visualizador del teléfono inteligente y la cámara que el fondo.

En esta coyuntura, se debe tener en cuenta que las realizaciones a modo de ejemplo anteriores para analizar las características de reflectividad de las imágenes capturadas por la cámara, con el fin de diferenciar entre una cara real y una fotografía o video de una cara, no están limitadas a dispositivos de teléfonos inteligentes, y se pueden aplicar a cualquier dispositivo con una fuente de luz y una cámara, tal como un ordenador portátil con una cámara web. Además, la frecuencia de la pulsación del visualizador (por ejemplo, el flash) podría ser cualquier frecuencia, y la duración de la medición se puede ajustar dependiendo de la confianza requerida de la medición. Además, se podría utilizar un medidor de lux para medir los niveles de luz ambiental y aumentar el tiempo de medición con

mucha luz, tal como la luz solar. El conocimiento de los niveles de luz ambiental también podría ser utilizado para ayudar a determinar la señal de potencia esperada. Por ejemplo, en iluminación media, el procesador configurado puede esperar la mayor intensidad de señal, en niveles de poca luz, el procesador configurado puede esperar que el pico de reflexión del ojo sature la cámara y causar una menor intensidad de señal y, en iluminación ambiental alta, el procesador configurado puede esperar que la intensidad de la señal se reduzca. Además, en algunas implementaciones, la fase de la señal de potencia en la región alrededor del ojo o en la totalidad de la cara podría ser verificada para ver si es compatible con lo esperado de la señal de pulsación del visualizador. Si la fase es compatible, indica que la luz ambiental es lo suficientemente baja como para que se detecte una buena señal desde la cara, si no es compatible, indica una señal débil y, por lo tanto, una alta iluminación ambiental. Esta información se puede utilizar en lugar de, o además de, como un medidor de lux.

En una realización adicional, la vitalidad se puede determinar detectando el movimiento de los rasgos faciales de nivel superior, por ejemplo, mediante la detección de una sonrisa. Los emparejadores de caras sin protección contra la vitalidad pueden ser engañados por impresiones fotográficas de alta resolución. Estas imágenes faciales están disponibles gratuitamente para casi cualquier persona en Internet. Un sistema de detección de sonrisas puede reconocer las expresiones faciales, por lo que puede solicitar al usuario que 'sonría para iniciar sesión'; esto es algo que una fotografía no puede hacer, lo que aumenta la seguridad del sistema contra intentos de suplantación de identidad.

En algunas implementaciones, las características del flujo óptico de las características de nivel bajo, medio y alto se pueden utilizar para detectar una sonrisa u otro movimiento facial similar. Por ejemplo, el procesador 110 del dispositivo móvil, que ejecuta uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172, y el módulo de análisis 174, puede analizar una secuencia de video de imágenes para determinar la vitalidad por medio de: encontrar la cara en las imágenes, a continuación, estabilizar los fotogramas de video de la región de la boca, después, dividir la boca en una región izquierda y derecha, y calcular el flujo óptico de cada región. En la transición a una sonrisa, el flujo óptico de las regiones izquierda y derecha se alejará en promedio uno de otro. El análisis del flujo óptico identifica de manera natural las esquinas y los bordes que están asociados con la boca y, por lo tanto, proporciona una manera eficiente de analizar el movimiento de la boca. En consecuencia, se puede detectar la vitalidad determinando que las características del flujo óptico de los rasgos faciales coinciden con el flujo óptico esperado de cualquier número de expresiones faciales. Alternativamente, se podría utilizar un algoritmo de cascada de Haar para detectar una sonrisa. Del mismo modo, se podría utilizar la detección de elevación de las cejas o la detección de un parpadeo.

De acuerdo con las realizaciones dadas a conocer, la detección de la mirada se puede utilizar para proporcionar una prueba de vitalidad discreta, solicitando al usuario que mueva los ojos de una manera concreta, y determinando si el movimiento de la mirada del usuario se mueve según lo solicitado. Por ejemplo, se le puede solicitar al usuario que “observe cómo se encienden las luces” y, a continuación, 3 bombillas (izquierda, central, derecha) se encienden aleatoriamente. Si el usuario mueve su mirada hacia cada bombilla correctamente mientras se iluminan, entonces pasa la prueba. Una fotografía no pasaría esta prueba, al igual que un video, debido a los movimientos específicos y aleatorios del iris que se solicitan. Esta prueba se podría utilizar en combinación con otras pruebas de vitalidad, tales como las pruebas de expresión facial o la detección de sonrisas. Dicha detección de la mirada se puede llevar a cabo utilizando los métodos a modo de ejemplo para detectar el movimiento de los rasgos faciales de nivel bajo, medio y alto descritos en relación con la figura 5, además de utilizar técnicas conocidas de visión por ordenador descritas, por ejemplo, en “In the Eye of the Beholder: A Survey of Models for Eyes and Gaze.”, publicado en: Pattern Analysis and Machine Intelligence, IEEE Transactions en (Volumen: 32, Edición: 3) y Biometrics Compendium, IEEE, fecha de publicación: marzo de 2010 Páginas: 478 a 500 ISSN: 0162-8828.

En una realización adicional, la vitalidad se puede determinar mediante la detección de signos vitales que están presentes en sujetos vivos. Cada vez que el corazón de un sujeto vivo late, la cara del sujeto late. Esta pulsación es tan pequeña que no puede ser detectada por los ojos humanos, pero puede ser capturada en imágenes, y ser detectada mediante el procesamiento de imágenes de la señal de video (por ejemplo, la secuencia de imágenes capturada utilizando la cámara de video). En consecuencia, de acuerdo con las realizaciones dadas a conocer, el dispositivo móvil puede ser configurado para determinar la vitalidad analizando las imágenes y determinando que el sujeto capturado tiene pulso. En algunas implementaciones, el procesador 110 del dispositivo móvil, que ejecuta uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172 y el módulo de análisis 174, puede estabilizar las imágenes de video capturadas por la cámara y utilizar algoritmos de detección de pulso para determinar la presencia de pulso en la secuencia de imágenes. Además o alternativamente, el procesador del dispositivo móvil configurado puede diferenciar entre fotografía y persona viva mediante la asignación de una amplitud de pulso, determinando la fuerza de la señal de pulso, determinando el color de la señal de pulso, determinando el nivel de ruido en el dominio de la frecuencia. Además, el procesador configurado también puede utilizar una segunda cámara del dispositivo móvil y LED para medir el pulso de un usuario en el dedo para ayudar a identificar el pulso en la cara, porque el pulso del dedo es más fiable. En consecuencia, utilizando el pulso medido desde el dedo, el procesador configurado puede identificar fácilmente todas las demás frecuencias de la cara como ruido. Algunos métodos alternativos para detectar el pulso de un sujeto a partir de imágenes se describen en el presente documento, y se pueden encontrar, por ejemplo, en “'Remote plethysmographic imaging using ambient light', Wim Verkruysse et al, Optics express, 22 de diciembre de 2008”.

Se puede suponer que el pulso del usuario es el componente de frecuencia más fuerte fisiológicamente viable de la señal; no obstante, una señal ruidosa de la de una fotografía también puede tener un pulso supuesto. En consecuencia, para la detección de la vitalidad, es preferible distinguir entre una señal de ruido de una fotografía y una señal de pulso genuina de una persona viva. De acuerdo con las realizaciones dadas a conocer, en algunas implementaciones, el procesador configurado puede distinguir entre una señal de ruido de una fotografía y una señal de pulso genuina comprobando la variación de la frecuencia de pulso supuesta a través de los datos. Por ejemplo, si se graban 20 segundos de datos de video, el procesador configurado puede calcular el pulso supuesto utilizando datos de 0 a 5 segundos, de 1 a 6 segundos, de 2 a 7 segundos, etc. Si la señal de pulso es genuina, el procesador configurado debe determinar que hay una baja variación entre cada una de estas mediciones; si la señal proviene de ruido, se espera una variación mayor. En consecuencia, esta información de variación puede ser utilizada por el procesador configurado para distinguir entre señales de vitalidad y de suplantación de identidad.

Del mismo modo, cuando un sujeto respira, su pecho se mueve, y este movimiento también puede ser detectado, para garantizar que el sujeto está respirando. En consecuencia, el dispositivo móvil configurado puede ser configurado para detectar intentos de suplantación de identidad mediante el análisis de las imágenes y la detección de dicho movimiento en el pecho para diferenciar entre un sujeto vivo y una reproducción estática (por ejemplo, una fotografía, que no mostrará dicho movimiento).

En una realización adicional, la vitalidad se puede determinar realizando un análisis tridimensional (3D) de las imágenes para verificar que las imágenes capturadas son de un sujeto vivo, que tiene una profundidad 3D, en lugar de una reproducción, en general, plana del sujeto (por ejemplo, utilizando un fotografía o visualizador de video).

De acuerdo con las realizaciones dadas a conocer, el procesador 110 del dispositivo móvil, que ejecuta uno o más módulos de software 130, que incluyen, preferiblemente, el módulo de captura 172, y el módulo de análisis 174, puede solicitar al usuario que realice un movimiento de exploración alrededor de su cara con la cámara del teléfono (por ejemplo, un escaneo de lado a lado, escaneo arriba y abajo y similares). Utilizando las imágenes capturadas, el procesador configurado puede utilizar técnicas de imágenes en 3D para construir un modelo del usuario en 3D. Mientras que las fotos y los videos son planos, un sujeto vivo no lo es. Al requerir que el objeto de autenticación tenga una forma de cara en 3D, es mucho más difícil suplantar la identidad para el sistema utilizando fotografías o videos.

El flujo óptico de píxeles medido y las características de una o más imágenes, por ejemplo, tal como se explicó anteriormente en relación con la figura 5, se puede utilizar para determinar la vitalidad en base a dicho análisis 3D. Imagínese mirando por el lado de un automóvil mientras viaja; los objetos en primer plano se mueven muy rápido porque están cerca, mientras que los objetos distantes parecen moverse más lentamente. De manera similar, una cámara de dispositivo móvil que se mueva más allá de una cara debe capturar imágenes que muestren que la nariz se mueve más rápido que los ojos y las orejas porque está más cerca. En consecuencia, el análisis del flujo óptico de la escena puede utilizar este movimiento relativo para deducir a qué distancia están los objetos capturados. Si el sujeto es una persona real, su nariz está más cerca del teléfono que sus ojos; sin embargo, si el sujeto es una fotografía o un video, entonces no lo está. Por lo tanto, la suplantación de identidad se puede detectar analizando el flujo óptico para detectar la distancia de diversos rasgos faciales de nivel bajo, medio y/o alto, o una combinación de los anteriores. Además, el dispositivo móvil configurado también puede verificar que el dispositivo móvil se está moviendo, y no que la cara gira, analizando el flujo óptico del fondo hacia la cara o los acelerómetros y/o la brújula en el dispositivo móvil.

Además del análisis 3D anterior que utiliza imágenes, además o alternativamente, se podría utilizar un sensor de profundidad basado en hardware para proporcionar información de profundidad sobre la cara. Por ejemplo, se podría utilizar un sensor de profundidad de luz estructurado como el utilizado en el sensor de profundidad Microsoft Kinect, comercializado por la firma Microsoft Inc. y el teléfono Google Tango, comercializado por la firma Google Inc. Del mismo modo, se podría utilizar un sensor de profundidad de tiempo de vuelo o una cámara estéreo. Utilizando dichos dispositivos, la vitalidad se puede deducir a partir de una sola imagen con un mapa de profundidad, y que es difícil falsificar una cara correctamente en tres dimensiones.

En algunas implementaciones, los mapas de profundidad de varias imágenes se podrían combinar para aumentar la precisión y/o extensión de la región asignada en profundidad. Además, se puede crear un mapa de profundidad utilizando la información de enfoque de la cámara óptica del dispositivo móvil. Si el enfoque se desplaza de cerca a lejos a medida que se recogen los fotogramas de video de la cara, la distancia de cada región desde la cámara se podría deducir identificando cuál de los fotogramas es el más nítido para esa región. Cuanto más cerca esté el fotograma más nítido de la región del comienzo de la secuencia del fotograma, más cerca de esa región de la imagen debe estar la cámara.

En algunas implementaciones, se puede producir una imagen de la cara como lo haría un mapa de profundidad. Durante la inscripción, se encontraría la cara, y la región correspondiente del mapa de profundidad se almacenaría con la imagen de la cara. Durante la autenticación, se puede probar la similitud de la imagen de la cara, y también se probaría la similitud de la forma de la cara, incluida la comparación del tamaño de la cara. La comparación podría implicar, en primer lugar, alinear el mapa de profundidad inscrito con el mapa de profundidad de prueba en las tres dimensiones utilizando técnicas tales como el punto iterativo más cercano (ICP - Iterative Closest Point, en inglés) y,

a continuación, evaluar la calidad de la coincidencia.

Otros dispositivos de hardware adicionales también podrían ser útiles para evaluar la vitalidad. Por ejemplo, es probable que las imágenes para suplantación de identidad aparezcan diferentes para una cámara infrarroja (cercana) con respecto a una cámara de espectro visible. Por ejemplo, los visualizadores de cristal líquido son, habitualmente, transparentes en el infrarrojo, y muchas tintas tienen una absorción diferente en el espectro infrarrojo. Los rostros humanos tienen ciertas características en el espectro infrarrojo que podrían ser confirmadas mediante la utilización de imágenes infrarrojas, por ejemplo, en el infrarrojo, los iris tienen una mayor reflectividad. A modo de ejemplo adicional, en el infrarrojo profundo, el perfil de temperatura de la cara se hace evidente. En consecuencia, el procesador configurado puede llevar a cabo la detección de vitalidad mediante la generación de un perfil de temperatura de un usuario y, a continuación, analizando el perfil de temperatura para confirmar que la cara tiene una temperatura esperada, o un patrón de temperatura de una cara humana, al contrario que un visualizador de video o fotografía. La temperatura esperada se puede determinar durante la inscripción y/o en base a las características conocidas de rostros humanos y a diversos métodos para representar el rostro de un humano, tal como se explicó anteriormente.

Resolución de imagen, análisis de histograma de intensidad, detección del movimiento ocular, detección de la frecuencia de escaneo de video y patrones de muaré de píxeles de video con los píxeles CCD de la cámara y reconocimiento de voz se pueden utilizar, asimismo, para distinguir entre imágenes de vitalidad y de suplantación de identidad. De acuerdo con esto, se puede apreciar que, de acuerdo con las realizaciones dadas a conocer, el procesador del dispositivo móvil configurado puede detectar la vitalidad, utilizando cualquier combinación de los métodos de detección de la vitalidad anteriores, a modo de ejemplo.

Los sistemas y métodos para autorizar el acceso a un entorno de acceso controlado no están limitados de ninguna manera a las realizaciones y/o disposiciones ilustradas, ya que las realizaciones y/o disposiciones ilustradas descritas son meramente a modo de ejemplo de los sistemas y métodos descritos en el presente documento, que pueden estar realizados en diversas formas, tal como aprecia un experto en la técnica. Algunas realizaciones disposiciones y aplicaciones a modo de ejemplo, alternativas, incluyen las siguientes realizaciones a modo de ejemplo.

En algunas implementaciones, un dispositivo móvil 101a de usuario configurado ejecutando uno o más módulos de software 130 de la aplicación de cliente de autenticación segura, por ejemplo, como una aplicación en segundo plano, puede determinar que el usuario 124 ha abierto otra aplicación que permite al usuario buscar para productos en Internet y realizar una compra en un ACE, por ejemplo, iTunes, comercializado por la firma Apple Inc. El procesador 110 del dispositivo móvil configurado también se puede configurar para determinar, a partir del perfil del usuario, que incluye las reglas de acceso / preferencias definidas por el usuario, introducidas durante la inscripción, que la aplicación particular es un ACE preferido. Como resultado, el procesador del dispositivo móvil puede iniciar de manera automática el proceso de autenticación, a modo de ejemplo, descrito en referencia a las figuras 3 a 5. Además o alternativamente, si las preferencias del usuario pueden especificar que el usuario prefiere iniciar sesión y autenticarse solo tras realizar una compra y el procesador del dispositivo móvil puede iniciar la autenticación biométrica en respuesta a que un usuario inicia la compra a través de la aplicación iTunes.

Para autorizar al usuario, el procesador del dispositivo móvil puede solicitar al usuario que escanee sus datos biométricos utilizando la cámara del dispositivo móvil. Entonces, el dispositivo móvil 101a y/o el servidor 105 del sistema pueden determinar: si el usuario está autenticado de manera biométrica, tiene una cuenta de iTunes y/o está autorizado para realizar la transacción utilizando la cuenta. Por ejemplo, el proceso de autenticación puede incluir autenticar de manera biométrica al usuario utilizando el dispositivo móvil, y transmitir desde el dispositivo móvil al servidor 105 del sistema una solicitud de transacción que identifica al usuario e incluye información sobre el ACE que requiere la autorización del usuario (por ejemplo, iTunes). Si los datos biométricos del usuario no están autenticados por el dispositivo móvil, o el usuario no está autorizado por el servidor 105 del sistema, el dispositivo móvil puede alertar al usuario con un tono. Tras una autenticación y autorización biométrica con éxito, el servidor 105 del sistema puede consultar el perfil de usuario creado durante la inscripción para recuperar información asociada con la cuenta de transacción del usuario (por ejemplo, la cuenta de iTunes) y transmitir una notificación de autorización que confirma la identidad del usuario e incluye la información de la cuenta de transacción del usuario necesaria para completar uno o más campos. La notificación de autorización puede ser transmitida al dispositivo móvil 101a, haciendo que el dispositivo móvil complete de manera automática los campos requeridos para completar el inicio de sesión del usuario y/o completar la compra de la canción según las preferencias del usuario.

En otra implementación a modo de ejemplo, un dispositivo informático 101b del usuario, que se ha inscrito en el sistema de autenticación segura (por ejemplo, un ordenador portátil personal) y se configura ejecutando la aplicación de cliente de autenticación segura, puede determinar que el usuario 124 ha abierto un navegador web y ha navegado a un sitio web de red social que requiere autenticación de usuario. El dispositivo informático también puede determinar a partir de un perfil de usuario almacenado localmente que el sitio web particular es un ACE al que se accede preferiblemente utilizando el sistema 100. El dispositivo informático también puede verificar la clave del sitio para garantizar que no se produzca una suplantación de identidad. En respuesta a la determinación de que el sitio web es un ACE preferido, el dispositivo informático 101b del usuario configurado puede iniciar el proceso de autorización transmitiendo una solicitud de autorización que identifica el sitio web y el usuario al servidor 105 del

sistema. En base a la solicitud de autorización, el servidor 105 del sistema puede localizar un perfil de usuario asociado con el usuario identificado e identificar un dispositivo móvil 101a inscrito que también está asociado con el usuario y/o el perfil de usuario. El servidor del sistema puede transmitir una solicitud de autenticación biométrica que hace que el dispositivo móvil identificado autentique de manera biométrica al usuario. Tras la autenticación biométrica del usuario, el dispositivo móvil puede transmitir una solicitud de transacción que confirma la autenticación e identifica al usuario y al dispositivo móvil 101a al servidor del sistema. Utilizando al menos la solicitud de transacción, el servidor del sistema puede autorizar al usuario a acceder al sitio web y transmitir una notificación de autorización al dispositivo informático 101b del usuario. En respuesta a la notificación de autorización, el dispositivo informático del usuario puede completar de manera automática los campos necesarios para completar el inicio de sesión del usuario, lo que facilita el acceso del usuario a su cuenta en línea. En algunas implementaciones, la notificación de autorización puede incluir la información de inicio de sesión del usuario recuperada de un perfil de usuario guardado en el servidor 105 del sistema. Además o alternativamente, la notificación de autorización puede solicitar al dispositivo de usuario 101b que recupere la información de inicio de sesión requerida desde una instancia del perfil de usuario almacenada por el dispositivo informático 101b.

En otra implementación a modo de ejemplo, un dispositivo informático 101b del usuario inscrito (por ejemplo, un ordenador portátil personal), que se configura ejecutando la aplicación de cliente de autenticación segura, puede determinar que el usuario ha abierto una aplicación de navegador y ha navegado a un proveedor de servicios de comunicaciones (por ejemplo, www.skype.com). El dispositivo informático 101b del usuario también puede determinar si las preferencias del perfil del usuario nombran al proveedor de servicios de pago como un ACE fiable y preferido, y también puede verificar la clave del sitio para garantizar una nula suplantación de identidad. A continuación, el dispositivo informático 101b del usuario puede iniciar el proceso de autorización para autorizar al usuario mediante el dispositivo móvil y el servidor del sistema de acuerdo con las realizaciones dadas a conocer. Tras la autorización, el servidor 105 del sistema puede transmitir una notificación de autorización, que incluye una clave fusionada exclusiva, de una sola utilización, al dispositivo informático 101b del usuario, y hacer que el dispositivo informático descifre de manera automática la clave fusionada utilizando una clave correspondiente almacenada por el dispositivo informático del usuario y complete los campos obligatorios necesarios para completar el inicio de sesión del usuario y permitir, de este modo, que el usuario obtenga acceso a su cuenta en línea. Por ejemplo, la clave puede estar basada en el identificador biométrico del usuario, en un identificador de usuario, en un identificador de dispositivo móvil o en una combinación de lo anterior.

A modo de ejemplo adicional, después de iniciar sesión, el usuario puede encontrar puntos de autorización adicionales, por ejemplo, si el usuario necesita comprar créditos para continuar utilizando el servicio y selecciona una opción de pago “PayPal”. Por consiguiente, el dispositivo informático 101b del usuario que ejecuta la aplicación de cliente de autenticación segura puede iniciar nuevamente la autorización del usuario transmitiendo una solicitud de autorización que identifica a PayPal como el ACE al servidor 105 del sistema. Tras la autorización del usuario de acuerdo con las realizaciones dadas a conocer, el servidor del sistema puede transmitir una notificación de autorización cifrada al dispositivo informático 101b del usuario que incluye la información de la cuenta PayPal del usuario, que el servidor del sistema almacena en el perfil del usuario, haciendo que el dispositivo informático complete la transacción completando de manera automática los campos obligatorios con la información de pago recibida y transmita la información a los servidores del lado del servidor asociados con el ACE (por ejemplo, paypal y/o skype).

En otra implementación a modo de ejemplo, las realizaciones descritas se pueden utilizar para facilitar el pago en un dispositivo informático 101b, que es un terminal transaccional asociado con una organización empresarial, por ejemplo, un terminal de punto de venta en un supermercado. En algunas implementaciones, el usuario puede iniciar una transacción de pago seleccionando, en el dispositivo móvil del usuario 101a, al supermercado concreto de una lista de vendedores preferidos almacenados en el perfil del usuario. En base a la selección del usuario, el dispositivo móvil 101a puede identificar las preferencias del usuario con respecto a las transacciones realizadas con el vendedor concreto. Por ejemplo, que el usuario prefiere realizar pagos utilizando una cuenta de tarjeta de crédito concreta identificada en el perfil del usuario, y también prefiere utilizar una cuenta del programa de fidelización al realizar compras. En consecuencia, una vez que el usuario toca un botón de pago en la interfaz de usuario del dispositivo móvil 115, el dispositivo móvil 101a puede solicitar al usuario que escanee sus datos biométricos y el dispositivo móvil y/o el servidor 105 del sistema pueden determinar si el usuario está autenticado de manera biométrica y autorizado para realizar un pago utilizando el método de pago concreto. Tras una autorización con éxito, el dispositivo móvil configurado que utiliza un transmisor NFC puede transmitir la información de pago del usuario y la información de la cuenta de fidelidad al dispositivo POS habilitado para NFC, pasando de este modo la información del usuario, la información de pago y el número de miembro de fidelización asociado con el usuario, para completar la transacción.

En otra implementación, el dispositivo de punto de venta (por ejemplo, el dispositivo informático 101b) puede recibir información de identificación del usuario desde el dispositivo móvil 101b, y puede transmitir una solicitud de autorización que incluye la información de la transacción (por ejemplo, precio, impuestos, etc.) e información de identificación del usuario y del vendedor concreto al servidor 105 del sistema. Utilizando la solicitud, el servidor del sistema puede identificar el dispositivo móvil 101a asociado con el usuario y hacer que el dispositivo móvil 101a solicite al usuario que se autentique de manera biométrica. Tras una autenticación biométrica con éxito por el dispositivo móvil 101a, el dispositivo móvil puede notificar al servidor 105 del sistema enviando una solicitud de

transacción que incluye una clave segura que identifica al usuario y al dispositivo móvil. Utilizando la clave, el servidor 105 del sistema puede identificar un perfil de usuario asociado con el usuario y el dispositivo móvil, e identificar una cuenta de pago para realizar la transacción especificada en la solicitud de autenticación. A continuación, el servidor 105 del sistema puede consultar un almacén de datos seguro mantenido por la organización empresarial que mantiene la cuenta de pago del usuario para recuperar la información de pago del usuario. El servidor del sistema puede procesar la transacción utilizando la información de pago y, una vez completada con éxito la transacción, el servidor 105 del sistema puede transmitir una notificación de autorización al dispositivo del punto de venta, indicando que la transacción fue procesada. Dicha implementación impide pasar información financiera y personal confidencial directamente al dispositivo POS del vendedor. Alternativamente, el servidor del sistema puede transmitir, al dispositivo POS, una notificación de autorización que incluye la información de pago, haciendo que el dispositivo POS o el sistema de procesamiento de pagos de los vendedores completen la transacción financiera.

En otra implementación, un dispositivo informático 101b que controla un punto de acceso seguro (el ACE, por ejemplo, un punto de control de seguridad del aeropuerto) puede ser configurado para comunicarse con dispositivos móviles habilitados y/o con el servidor 105 del sistema. En algunas implementaciones, el dispositivo informático del punto de acceso 101b puede transmitir una solicitud de autorización directamente al dispositivo móvil habilitado por el usuario 101a. En respuesta a la recepción de la solicitud, el dispositivo móvil 101a, que se configura ejecutando la aplicación de cliente de autenticación segura, puede autenticar de manera biométrica al usuario. Tras la autenticación, el dispositivo móvil puede transmitir una solicitud de transacción al servidor 105 del sistema que identifica el dispositivo informático 101b, el usuario y el dispositivo móvil. En respuesta a la solicitud de transacción, el servidor 105 del sistema puede autorizar al usuario verificando la identidad del usuario y autorizando el paso a través del punto de acceso de acuerdo con las reglas de acceso del usuario recopiladas del perfil de usuario o de un almacén de datos seguro. Por ejemplo, las reglas pueden referirse a restricciones de viaje (por ejemplo, si el viajero no está en una lista de exclusión aérea) guardadas en una base de datos del gobierno. Si el servidor 105 del sistema determina que la identidad del usuario no se ha verificado, o las reglas de acceso indican que el usuario tiene restringido el viaje, se puede transmitir una notificación de autorización al dispositivo móvil 101a para alertar al usuario. El servidor 105 del sistema también puede transmitir una notificación de autorización al dispositivo informático 101b que controla el acceso al ACE, por ejemplo, para impedir el acceso del usuario y/o alertar a un guardia de seguridad a través de un visualizador. De manera similar, tras una autenticación con éxito, el dispositivo móvil 101a y el dispositivo informático del punto de acceso 101b pueden ser notificados de manera similar. Además, el servidor 105 del sistema también puede transmitir información del usuario, por ejemplo, un nombre y una imagen del usuario 124 al dispositivo informático 101b, para una autorización adicional, si es necesario. La notificación de autorización también puede hacer que el dispositivo informático del punto de acceso permita al usuario 124 pasar físicamente a través del punto de control de seguridad, por ejemplo, abrir una puerta que permita al usuario caminar hacia su puerta y esperar a embarcar.

En otra implementación, el dispositivo informático 101b puede ser un punto de acceso controlado electrónicamente (por ejemplo, una cerradura electrónica en red) en una puerta segura configurada para comunicarse con dispositivos móviles habilitados 101a y con el servidor 105 del sistema. El dispositivo informático del punto de acceso 101b puede transmitir una solicitud de autenticación directamente al dispositivo móvil 101a haciendo que el dispositivo móvil 101a comience el proceso de autorización. Alternativamente, el dispositivo móvil 101a puede transmitir un mensaje que identifica al usuario y al dispositivo móvil directamente al dispositivo informático del punto de acceso 101b, lo que provoca que el punto de acceso transmita una solicitud de autorización al servidor 105 del sistema, que identifica al usuario y al punto de acceso. Mediante la utilización de la solicitud, el servidor 105 del sistema puede consultar el perfil de usuario asociado con el usuario para identificar el dispositivo móvil y transmitir una solicitud de autenticación biométrica que hace que el dispositivo móvil 101a comience el proceso de autenticación biométrica. Tras una autenticación con éxito, el servidor 105 del sistema puede determinar a partir de las reglas de acceso asociadas con el dispositivo informático 101b del punto de verificación concreto si el usuario está autorizado para acceder al área segura y, de ser así, transmitir una notificación de autorización al dispositivo informático 101b que hace que el punto de verificación desbloquee la puerta.

En algunas implementaciones, el dispositivo informático del usuario (por ejemplo, 101b) puede ser un terminal de transacción, por ejemplo, un cajero automático, configurado para interactuar con el servidor 105 del sistema. El cajero automático se puede configurar, además, para comunicarse con el dispositivo móvil habilitado del usuario 101a, por ejemplo, transmitiendo información al dispositivo móvil 101a cuando el dispositivo móvil está dentro de un rango definido. Tras la recepción de la comunicación del cajero automático, el dispositivo móvil 101a puede iniciar el proceso de autenticación solicitando al usuario 124 que se autentique. El dispositivo móvil 101a puede capturar y autenticar los datos biométricos del usuario y notificarlo al servidor del sistema tal como se describe en relación con las figuras 3 y 4. En consecuencia, el dispositivo móvil 101a y/o el servidor 105 del sistema pueden determinar si el usuario está autenticado de manera biométrica y determinar si el usuario está autorizado para utilizar el cajero automático (por ejemplo, tiene una cuenta o cuentas de transacción a las que se puede acceder utilizando el cajero automático). Además, el dispositivo móvil y/o el servidor del sistema pueden consultar bases de datos fiables guardadas en el servidor 105 del sistema, o una base de datos corporativa (por ejemplo, el dispositivo informático remoto 102, que es, por ejemplo, operado por un banco) para realizar controles de seguridad adicionales de acuerdo con la identidad del usuario, para garantizar que el usuario no tenga restricciones para realizar transacciones, por

ejemplo, en una lista AML (anti-blanqueo de dinero) o de vigilancia. Si el usuario no está autenticado y/o carece de permisos para realizar la transacción, se puede alertar al usuario a través del dispositivo móvil 101a. Además, el banco (por ejemplo, el dispositivo informático remoto 102) o el cajero automático (por ejemplo, el dispositivo informático 101b) pueden recibir notificaciones de error o intento de fraude. Si está autorizado, el servidor 105 del sistema puede transmitir una notificación de autorización al cajero automático 101b y/o a una red bancaria asociada para avanzar la transacción en el cajero automático. Por ejemplo, avanzar en la transacción puede incluir autorizar la transacción solicitada, mostrar opciones de usuario (por ejemplo, retirar efectivo, transferir fondos, verificar saldo, etc.), solicitar más información del usuario en favor de la transacción y similares, tal como lo comprenderían los expertos en la técnica. De esta manera, las realizaciones dadas a conocer pueden eliminar la necesidad de tarjetas de transacción y números PIN y pueden prevenir el fraude. Además, dicho sistema puede eliminar la necesidad de números de cuenta de usuario arbitrarios.

En otra implementación a modo de ejemplo, el servidor 105 del sistema y/o uno o más servidores y dispositivos de almacenamiento conectados de manera comunicativa al mismo, pueden ser configurados para alojar una plataforma de comunicación y de utilización compartida de archivos cifrados. Se puede apreciar que la plataforma de intercambio de archivos cifrados no se limita al almacenamiento o la transmisión de archivos de datos cifrados en el sentido tradicional, y puede ser aplicable a la transmisión de cualquier paquete electrónico de datos. Por ejemplo, la plataforma de intercambio encriptada puede ser configurada para permitir a los usuarios proteger y transmitir correos electrónicos, archivos adjuntos de cualquier tamaño, chat de texto, llamadas de voz (VoIP), videollamadas, mensajes de grupo y similares.

De manera más específica, los dispositivos de usuarios inscritos que ejecutan la aplicación de autenticación segura se pueden configurar para transmitir mensajes cifrados a otros usuarios inscritos a través del servidor 105 del sistema. Tal como se señaló anteriormente, preferiblemente, todas las comunicaciones entre un dispositivo de usuario inscrito y el servidor del sistema se pueden enviar a través de un entorno de comunicación seguro, SSL, en dos direcciones, utilizando una clave que fue generada durante la inscripción en base, por ejemplo, al identificador biométrico del usuario, de otro usuario y/o a identificadores de dispositivo y/o claves generadas durante la inscripción, o una combinación de los anteriores. La utilización de una clave asimétrica realizada de los propios datos biométricos de los usuarios proporciona una clave que es única para el usuario y, de este modo, se puede utilizar para afirmar la identidad del usuario. Preferiblemente, la clave está cifrada, adicionalmente, utilizando un cifrado de curva elíptica de 384 bits. En consecuencia, las claves generadas, la información biométrica, los datos y otra información cifrada utilizando las claves también resultan prácticamente ilegibles, excepto para el servidor del sistema.

Además, el servidor del sistema también puede recibir reglas introducidas por los usuarios utilizando los dispositivos informáticos de los usuarios inscritos (por ejemplo, el dispositivo informático 101b y/o el dispositivo móvil 101a). Por ejemplo, las reglas recibidas del usuario pueden identificar al menos a otro usuario inscrito que esté aprobado para recibir o tener acceso a los archivos cifrados o a las transmisiones de datos. En consecuencia, el servidor del sistema puede mantener registros de las relaciones entre los usuarios del sistema, y facilitar el intercambio seguro de datos entre usuarios autenticados que están autorizados de acuerdo con las reglas de acceso.

Por ejemplo, un usuario puede iniciar una sesión de transferencia de datos cifrados utilizando el dispositivo móvil 101a y designar a otro usuario como el destinatario previsto. En consecuencia, el servidor del sistema puede hacer que el usuario remitente se autentique de manera biométrica utilizando el dispositivo móvil. Si el usuario remitente se autentica de manera biométrica, se puede establecer una conexión de SSL / TLS bidireccional entre el servidor del sistema y el dispositivo móvil para cada una de dichas transacciones (por ejemplo, de sesión o transmisión), tal como se explicó anteriormente. Una vez que se crea esta conexión segura, todos los datos enviados por el usuario a través de la capa SSL / TLS pueden ser cifrados utilizando la clave anteriormente generada durante la inscripción. Esto proporciona un método de transporte robusto y seguro para todos los tipos de datos entre el dispositivo emisor y el servidor del sistema.

Un aspecto destacado de la plataforma de intercambio de archivos es que requiere autenticación biométrica y afirmación de identidad para transmitir / almacenar / recibir o acceder a la información encriptada, proporcionando de este modo un alto nivel de protección y seguridad para la información a medida que pasa de un usuario a otro usuario a través del servidor del sistema. El único dispositivo con la capacidad de descifrar los mensajes es el servidor del sistema que contiene el algoritmo general utilizado para cifrar y descifrar mensajes y gestiona el entorno de comunicaciones seguras de SSL de dos direcciones con los dispositivos de los usuarios. En el caso de que este algoritmo se hiciera público, los datos de cada usuario siguen siendo seguros, porque no es necesario que los datos del usuario residan en el servidor del sistema y toda la información puede residir con el usuario en sus dispositivos, y solo con una autenticación biométrica válida, bajo una conexión de SSL de dos direcciones válida puede comunicar la información entre los dispositivos del usuario y el servidor del sistema.

Tras la recepción del mensaje cifrado del usuario emisor y, de acuerdo con las reglas de acceso asociadas, el servidor del sistema puede reenviar el mensaje de manera segura al destinatario previsto o transmitir una notificación al destinatario previsto informándole de que un mensaje seguro está esperando a ser entregado. En concreto, el servidor del sistema puede requerir que el destinatario esté autenticado y autorizado de manera biométrica y, si tiene éxito, el servidor del sistema puede descifrar el mensaje. Además, el servidor del sistema

puede establecer una sesión de comunicación de SSL de dos direcciones con el dispositivo del destinatario para reenviar el mensaje al destinatario de manera segura.

Se puede apreciar que la plataforma de intercambio de archivos cifrados no está limitada a compartir archivos de datos cifrados en el sentido tradicional y puede ser aplicable a la transmisión de cualquier mensaje electrónico. En algunas implementaciones, la plataforma de intercambio cifrado se puede configurar para permitir a los usuarios proteger y transmitir: correo electrónico, chat de texto, llamadas de voz (VoIP), videollamadas, mensajes de grupo utilizando cualquiera de los anteriores, archivos adjuntos de cualquier tamaño. Además, la plataforma se puede configurar para realizar otras funciones conocidas de la plataforma, tales como la traducción de mensajes, por ejemplo, utilizando Google Translate de Google Inc.

En algunas implementaciones, el servidor 105 del sistema puede incluir un servidor de correo cifrado que puede estar situado entre un servidor de correo corporativo y el resto del mundo, de tal manera que está diseñado para descifrar y cifrar todo el correo saliente de un usuario inscrito que está destinado a otro usuarios designados De esta manera, la integración puede ser muy simple para cualquier organización, sin necesidad de que modifiquen o reemplacen su servidor de correo existente (excepto para reenviar todo el correo al servidor de correo seguro).

Se puede apreciar que, en algunas implementaciones, el servidor 105 del sistema también puede mantener un historial de autorizaciones de un usuario utilizando el sistema, incluida toda la información recopilada y/o procesada durante los procesos a modo de ejemplo de autenticación y autorización biométrica. Por ejemplo, el servidor del sistema puede almacenar registros y detalles relativos a transacciones financieras, compras, etc. realizadas por el usuario de acuerdo con las realizaciones dadas a conocer en una o más bases de datos, creando de este modo una pista de auditoría financiera para el usuario. Se debe comprender que la información relativa a todas y cada una de las solicitudes de acceso, transacciones y actividad puede ser almacenada por el servidor 105 del sistema.

Por ejemplo, el servidor 105 del sistema puede almacenar un registro de las sesiones de autorización de un usuario, que pueden incluir GPS y otros datos de ubicación física similares, creando de este modo una pista de auditoría física del usuario. Además, se puede solicitar periódicamente al usuario que se autentique con el servidor del sistema simplemente con el fin de registrar la ubicación personal del usuario de manera autenticada. Los registros de auditoría física y financiera almacenados pueden ser accesibles para el usuario a través de dispositivos informáticos que están configurados para interactuar con el servidor 105 del sistema. Por ejemplo, utilizando una interfaz similar a un tablero de instrumentos presentada por un dispositivo móvil 101a inscrito o un dispositivo informático 101b que ejecuta la aplicación de autenticación segura o mediante una interfaz de usuario basada en la web. Utilizando el tablero de instrumentos, el usuario puede ajustar la configuración, las preferencias y especificar las reglas de acceso para las pistas de auditoría (por ejemplo, física, financiera y similares). Por ejemplo, el usuario 124 puede revisar y especificar otras personas y organizaciones que están autorizadas a tener acceso a los datos de seguimiento de la auditoría del usuario, o partes específicas de los registros de auditoría. Además, el usuario puede conceder acceso condicional a la organización / persona especificada de acuerdo con los términos del usuario, que incluyen, entre otros, restricciones de utilización y coste.

En algunas implementaciones, la información de ubicación por GPS del usuario puede ser recopilada por el dispositivo móvil 101a del usuario o por cualquier otro dispositivo informático habilitado para GPS (por ejemplo, el dispositivo informático 101b) que está asociado con el usuario y/o un entorno de acceso controlado al que accede el usuario de acuerdo con las realizaciones dadas a conocer. El servidor 105 del sistema puede almacenar la información de utilización y ubicación en uno o más almacenes de datos asociados. Por ejemplo, un dispositivo informático 101b habilitado para GPS puede estar ubicado en el automóvil del usuario y recopilar información de ubicación del GPS acerca de la ubicación del automóvil. La información de ubicación puede ser transmitida al servidor 105 del sistema o directamente a una base de datos para mantener una pista de auditoría física de los datos del GPS para el automóvil y el dispositivo informático 101b.

A modo de ejemplo adicional en algunas implementaciones, el servidor 105 del sistema también puede controlar el acceso / utilización del dispositivo informático 101b y/o un ACE asociado (por ejemplo, el vehículo), de acuerdo con las realizaciones dadas a conocer. Por ejemplo, al requerir autenticación biométrica / autorización del usuario antes de proporcionar acceso al dispositivo informático o vehículo o restringir el acceso de otra manera.

Los datos de ubicación se pueden utilizar para varios propósitos, por ejemplo y sin limitación, rastrear el movimiento de vehículos de la flota, monitorizar la utilización, rastrear vehículos robados y similares. Por consiguiente, se puede apreciar que, en algunos casos, es deseable controlar y compartir la información de ubicación recopilada por el dispositivo informático 101b y el vehículo asociado. Sin embargo, en vista de las preocupaciones de privacidad, los usuarios pueden no querer rastrear la ubicación a menos que sea necesario. A la vista de dichas preocupaciones de privacidad, en algunas implementaciones, el usuario 124 puede especificar reglas que definen el alcance de la información de ubicación, por ejemplo, del dispositivo informático 101b, o de un dispositivo móvil 101a u otros dispositivos informáticos (por ejemplo, un dispositivo de rastreo de ubicación de automóvil, exclusivo) que se debe recopilar o poner a disposición para su monitorización por individuos / sistemas corporativos. Por ejemplo, el usuario 124 puede especificar que no desea compartir la información de ubicación del usuario que se recopila mientras el usuario está en el vehículo, pero desea que la ubicación sea monitorizada mientras el usuario no está en el automóvil (por ejemplo, con fines de rastreo de robo del automóvil). A modo de ejemplo adicional, si administra una

flota de automóviles y empleados, un usuario 124 puede especificar que desea rastrear la ubicación de un vehículo, incluido el dispositivo informático 101b, cuando un empleado está en el automóvil.

En algunas implementaciones, cuando se interactúa con el dispositivo informático 101b (por ejemplo, activado por un usuario, alguien enciende el automóvil haciendo que el dispositivo informático 101b comience a recopilar información de ubicación y similares), el dispositivo informático puede escanear los datos biométricos del usuario y autenticar de manera biométrica al usuario de acuerdo con las realizaciones dadas a conocer. Además o alternativamente, el dispositivo informático 101b puede transmitir una solicitud de autorización al servidor 105 del sistema. La solicitud de autorización puede identificar el dispositivo informático 101b y también puede incluir información adicional, por ejemplo, una ubicación de GPS del dispositivo informático, una identidad del usuario, etc. En respuesta a la solicitud, el servidor del sistema puede determinar, a partir de la información recibida y de perfiles de usuario almacenados, que el dispositivo informático 101b está asociado con un usuario 124, y solicita a un dispositivo móvil asociado 101a que autentique al usuario. A modo de ejemplo adicional, si varios usuarios tienen acceso al vehículo que tiene un dispositivo de rastreo (por ejemplo, el dispositivo informático 101b), se le puede solicitar al usuario que se identifique con el dispositivo informático 101b para obtener autorización antes o después de acceder al automóvil. Por consiguiente, la solicitud de autenticación puede identificar al usuario concreto, de tal manera que el servidor del sistema puede solicitar al dispositivo móvil 101a del usuario apropiado que autentique de manera biométrica al usuario. Además o alternativamente, el servidor 105 del sistema puede realizar una notificación a todos los usuarios aprobados, de tal manera que el usuario apropiado pueda continuar la autenticación. Además o alternativamente, en función de la ubicación del dispositivo informático 101b, el servidor del sistema puede identificar un dispositivo móvil registrado que tenga una ubicación correspondiente y solicitar al usuario asociado que se autentique.

En algunas implementaciones, el usuario puede iniciar el proceso de autenticación utilizando el dispositivo informático 101b y/o el dispositivo móvil 101a del usuario. Por ejemplo, cuando el usuario se sube a un automóvil que tiene un dispositivo informático 101b, el usuario puede iniciar el proceso de autenticación, de tal manera que la ubicación del usuario no sea rastreada por el dispositivo móvil 101a o por el dispositivo informático 101b. Además o alternativamente, se le puede solicitar al usuario que se autentique antes de que se le permita acceder / activar el automóvil asociado con el dispositivo informático 101b (por ejemplo, arrancar el automóvil).

Siempre que la identidad del usuario esté autenticada, el servidor 105 del sistema puede conceder acceso al ACE (por ejemplo, al dispositivo informático, al automóvil y similares) o recopilar / proporcionar acceso a la información registrada por esos dispositivos de acuerdo con las reglas de acceso asociadas con el usuario 124, el dispositivo móvil 101a, el dispositivo informático 101b, el ACE y similares, por ejemplo, si las preferencias del usuario especifican que un cónyuge puede acceder a la información de ubicación del usuario, pero no debe ser compartida con una empresa de rastreo de robos, el servidor 105 del sistema puede conceder acceso al cónyuge y denegar el acceso a la empresa de rastreo de robos. A modo de ejemplo adicional, si el propietario de un automóvil especifica en la configuración asociada con el dispositivo informático 101b, que un usuario concreto tiene acceso al automóvil entre las 8 AM y las 11 PM y que la ubicación debe ser monitorizada de manera continua mientras está en utilización por el usuario concreto, el servidor del sistema puede permitir, después de una autenticación / autorización con éxito, que el usuario concreto acceda al automóvil durante la ventana de tiempo especificada, pueda monitorizar de manera continua la ubicación mientras está en utilización y también pueda proporcionar acceso a la información de ubicación al propietario.

En esta coyuntura, se debe tener en cuenta que, aunque gran parte de la descripción anterior se ha dirigido a sistemas y métodos para autorizar a un usuario a acceder a un entorno de acceso controlado de acuerdo con las características biométricas del usuario, los sistemas y métodos descritos en el presente documento pueden ser desplegados y/o implementados de manera similar en escenarios, situaciones y entornos mucho más allá de los escenarios referenciados.

Si bien esta especificación contiene muchos detalles de implementación específicos, estos no deben ser interpretados como limitaciones en el alcance de cualquier implementación o de lo que se puede afirmar, sino más bien como descripciones de características que pueden ser específicas para realizaciones concretas de implementaciones concretas. Ciertas características que se describen en la presente memoria descriptiva en el contexto de realizaciones separadas también pueden ser implementadas en combinación en una sola realización. Por el contrario, varias características que se describen en el contexto de una sola realización también pueden ser implementadas en múltiples realizaciones por separado o en cualquier subcombinación adecuada. Además, aunque las características se han podido describir anteriormente como que actúan en ciertas combinaciones, e incluso reivindicar inicialmente como tales, una o más características de una combinación reivindicada pueden ser eliminadas, en algunos casos, de la combinación, y la combinación reivindicada puede dirigirse a una subcombinación o variación de una subcombinación.

De manera similar, aunque las operaciones se representan en los dibujos en un orden concreto, esto no se debe comprender como que requiere que dichas operaciones se realicen en el orden concreto mostrado o en orden secuencial, o que todas las operaciones ilustradas sean llevadas a cabo, para conseguir resultados deseables. En ciertas circunstancias, el procesamiento en multitarea y en paralelo puede ser ventajoso. Además, no se debe comprender que la separación de diversos componentes del sistema en las realizaciones descritas anteriormente

requiera dicha separación en todas las realizaciones, y se debe comprender que los componentes y sistemas del programa descritos pueden ser integrados conjuntamente, en general, en un solo producto de software, o estar empaquetados en múltiples productos de software.

La terminología utilizada en el presente documento tiene el propósito de describir solamente realizaciones concretas, y no pretende ser limitativa de la invención. Tal como se utiliza en el presente documento, las formas singulares “un”, “una” y “el”, “la” están destinadas a incluir también las formas plurales, a menos que el contexto indique claramente lo contrario. Se comprenderá, además, que los términos “comprende” y/o “que comprende”, cuando se utilizan en la presente memoria descriptiva, especifican la presencia de características, números enteros, etapas, operaciones, elementos y/o componentes establecidos, pero no excluyen la presencia o la adición de una o más características, números enteros, etapas, operaciones, elementos, componentes y/o grupos de los mismos. Se debe observar que la utilización de los términos ordinales tales como “primero”, “segundo”, “tercero”, etc., en las reivindicaciones para modificar un elemento de la reivindicación no connota por sí mismo ninguna prioridad, precedencia u orden de un elemento de la reivindicación sobre otro o el orden temporal en el que se llevan a cabo los actos de un método, sino que se utilizan simplemente como etiquetas para distinguir un elemento de la reivindicación que tiene un nombre determinado de otro elemento que tiene el mismo nombre (pero para la utilización del término ordinal) para distinguir los elementos de la reivindicación. Además, la fraseología y la terminología utilizadas en el presente documento tienen fines descriptivos y no deben ser considerados como limitativos. La utilización de “que incluye”, “que comprende” o “que tiene”, “que contiene”, “que implica” y sus variaciones en el presente documento, pretende abarcar los elementos enumerados a continuación y sus equivalentes, así como elementos adicionales. Se debe comprender que números iguales en los dibujos representan elementos similares a través de las diferentes figuras, y que no todos los componentes y/o etapas descritos e ilustrados con referencia a las figuras son necesarios para todas las realizaciones o disposiciones.

Por lo tanto, las realizaciones y disposiciones ilustrativas de los presentes sistemas y métodos proporcionan un método implementado por ordenador, un sistema informático y un producto de programa informático para autorizar a un usuario a acceder a un entorno de acceso controlado. El diagrama de flujo y los diagramas de bloques en las figuras ilustran la arquitectura, la funcionalidad y el funcionamiento de posibles implementaciones de sistemas, métodos y productos de programas informáticos de acuerdo con diversas realizaciones y disposiciones. A este respecto, cada bloque en el diagrama de flujo o en los diagramas de bloques puede representar un módulo, segmento o porción de código, que comprende una o más instrucciones ejecutables para implementar las funciones lógicas especificadas. Asimismo, se debe tener en cuenta que, en algunas implementaciones alternativas, las funciones indicadas en el bloque pueden ocurrir fuera del orden indicado en las figuras. Por ejemplo, dos bloques mostrados en sucesión pueden, de hecho, ser ejecutados de manera sustancialmente simultánea, o los bloques a veces pueden ser ejecutados en el orden inverso, dependiendo de la funcionalidad involucrada. También se observará que cada bloque de los diagramas de bloques y/o la ilustración del diagrama de flujo, y las combinaciones de bloques en los diagramas de bloques y/o la ilustración del diagrama de flujo, pueden ser implementados mediante sistemas basados en hardware de propósito especial que realizan las funciones o actos especificados, o combinaciones de hardware de propósito especial e instrucciones informáticas.

El tema descrito anteriormente se proporciona solo a modo de ilustración, y no debe ser interpretado como limitativo. Se pueden realizar diversas modificaciones y cambios en el asunto descrito en el presente documento, sin seguir las realizaciones a modo de ejemplo y las aplicaciones ilustradas y descritas, y sin apartarse del alcance de la presente invención.

REIVINDICACIONES

1. Un método para autorizar el acceso a un entorno de acceso controlado (100), que comprende:

inscripción (300), por un dispositivo informático (105) que tiene un medio de almacenamiento (290) que tiene instrucciones almacenadas en el mismo y un procesador (210) configurado mediante la ejecución de las instrucciones en el mismo, de una pluralidad de usuarios (124), en el que, para cada uno de la pluralidad de usuarios, la inscripción incluye:

recepción, por el dispositivo informático de un dispositivo móvil respectivo, una aplicación de capa de puertos seguros, SSL, de dos direcciones, un certificado y una interfaz de programación de aplicaciones, API, una clave que identifica de manera única una aplicación de autenticación biométrica concreta que se ejecuta en el dispositivo móvil respectivo, en el que el dispositivo móvil respectivo es un dispositivo informático móvil, personal, del usuario respectivo;

establecimiento, mediante el dispositivo informático, de una sesión de comunicación segura inicial con el dispositivo móvil respectivo en base al certificado de SSL de dos direcciones de la solicitud recibida, que recibe, mediante el dispositivo informático del dispositivo informático del usuario durante la sesión inicial de comunicación segura, información de identificación asociada con el usuario respectivo y el dispositivo móvil respectivo; causando, durante la sesión de comunicación segura inicial, la asignación de una clave respectiva, tras la confirmación de la identidad de un usuario respectivo en base a los datos biométricos, la información de identificación asociada con el usuario respectivo y el dispositivo móvil (101a) respectivo, en el que la clave respectiva es una clave cifrada de SSL de dos direcciones con una capa de puertos seguros, que es adecuada para identificar de manera exclusiva al usuario respectivo emparejado con el dispositivo móvil respectivo y establecer sesiones de comunicación seguras posteriores entre el dispositivo móvil respectivo y el dispositivo informático,

almacenar la clave respectiva en al menos una base de datos (280) en asociación con un perfil de usuario respectivo, en el que los perfiles de usuario respectivos están asociados con cuentas de usuario respectivas que están asociadas con entornos de control de acceso respectivos, y en el que una clave privada respectiva, que corresponde a la clave respectiva, es proporcionada en el dispositivo móvil respectivo y almacenada en el dispositivo móvil respectivo durante la inscripción, y en el que la clave privada respectiva es una clave cifrada de SSL de dos direcciones que es adecuada para identificar de manera única al usuario respectivo emparejado con el dispositivo móvil y establecer sesiones de comunicación seguras entre el dispositivo móvil respectivo y el dispositivo informático;

recepción, por el dispositivo informático (105), de información de control de acceso que identifica el entorno de acceso controlado (100);

recepción, por el dispositivo informático (105) desde un dispositivo móvil (101a) a través de una red, de una solicitud de transacción que comprende una o más transmisiones e incluye: a) una clave privada respectiva, en la que la clave privada respectiva es adecuada para identificar a un usuario (124) emparejado con el dispositivo móvil (101a), y b) un indicador que indica si el usuario ha sido autenticado por el dispositivo móvil en base a los datos biométricos del usuario; procesamiento, mediante el dispositivo informático (105), utilizando al menos una base de datos (280), de la solicitud de transacción, en la que el procesamiento incluye:

verificar que la clave privada respectiva recibida corresponde a una clave respectiva almacenada en un perfil de usuario y, en base a la verificación, establecer una sesión de comunicación cifrada entre el dispositivo móvil (101a) y el dispositivo informático (105) utilizando la clave privada respectiva,

verificar que el indicador confirma que la identidad del usuario ha sido autenticada por el dispositivo móvil en base a los datos biométricos del usuario,

verificar que una o más transmisiones se ajusten a una configuración predeterminada, y

autorización, por el dispositivo informático (105), en base al procesamiento de la solicitud de transacción, al usuario (124), para acceder al entorno de acceso controlado (100), mediante la determinación de que el perfil de usuario correspondiente a la clave privada respectiva identifica una cuenta de transacción que está asociada con el entorno de acceso controlado;

generación, por el dispositivo informático (105), de una notificación de autorización que facilita al usuario autorizado el acceso al entorno de acceso controlado (100); y

transmisión, por el dispositivo informático (105) al menos a un dispositivo informático remoto a través de una red, de la notificación de autorización.

2. El método de la reivindicación 1, en el que la solicitud de transacción comprende una pluralidad de

transmisiones, y en el que la etapa de verificar que la clave privada respectiva corresponde a la clave respectiva comprende:

verificar que la clave privada respectiva proporcionada en la pluralidad de transmisiones corresponde a la clave respectiva almacenada en el perfil del usuario.

3. El método de cualquiera de las reivindicaciones 1 a 2 anteriores, en el que la etapa de verificar que una o más transmisiones se ajustan a una configuración predeterminada comprende:

determinar que una o más transmisiones difieren de una manera prescrita de una transmisión previa.

4. El método de cualquiera de las reivindicaciones 1 a 3 anteriores, en el que la etapa de verificar que una o más de las una o más transmisiones se ajusta a una configuración predeterminada comprende:

determinar que el indicador que confirma que la identidad del usuario ha sido autenticado por el dispositivo móvil (101a) en base a los datos biométricos, se recibió dentro de un plazo predefinido.

5. El método de cualquiera de las reivindicaciones 1 a 4 anteriores, en el que la información de control de acceso identifica adicionalmente al usuario (124), y comprende, además:

procesamiento, por el dispositivo informático (105), de la información de control de acceso para:

identificar en la al menos una base de datos (280) al menos un perfil de usuario que identifica al usuario; e

identificar el dispositivo móvil (101a) en al menos un perfil de usuario;

generación, por el dispositivo informático (105), de una solicitud de autenticación biométrica que facilita la autenticación biométrica del usuario; y transmisión, por el dispositivo informático (105) al dispositivo móvil (101a) a través de la red, de la solicitud de autenticación biométrica para que el dispositivo móvil autentique de manera biométrica al usuario.

6. El método de cualquiera de las reivindicaciones 1 a 5 anteriores, en el que verificar que la indicación confirma que la identidad del usuario ha sido autenticada por el dispositivo móvil (101a) en base a los datos biométricos del usuario comprende:

determinar que al menos una de las una o más transmisiones incluye el indicador que confirma que el usuario ha sido autenticado por el dispositivo móvil (101a) en base a los datos biométricos.

7. El método de cualquiera de las reivindicaciones 1 a 6 anteriores, en el que el perfil del usuario incluye información de la cuenta de transacción relacionada con la cuenta de la transacción, y en el que al menos una base de datos (280) incluye al menos una regla de acceso que restringe el acceso al entorno de acceso controlado (100); y que comprende, además:

recuperación, por el dispositivo informático (105) de la al menos una base de datos (280) en base al menos a la información de control de acceso, de la al menos una regla de acceso;

recuperación, por el dispositivo informático (105) del perfil de usuario, de la información de la cuenta de transacción; y

en el que el usuario (124) está autorizado, además, para acceder al entorno de acceso controlado (100) en base a la información de la cuenta de la transacción y a la al menos una regla de acceso.

8. El método de cualquiera de las reivindicaciones 1 a 7 anteriores, en el que el al menos un dispositivo informático remoto está asociado con el entorno de acceso controlado.

9. El método de cualquiera de las reivindicaciones 1 a 7 anteriores,

en el que el al menos un dispositivo informático remoto uno o más de asociado con el usuario (124) y el dispositivo móvil (101a); y

en el que la notificación de autorización incluye información que otorga al menos un dispositivo informático acceso al entorno de acceso controlado (100); o

en el que la notificación de autorización hace que al menos un dispositivo informático remoto:

recupere, de una memoria de acuerdo con la notificación de autorización, los detalles de la cuenta asociados con al menos una cuenta de transacción, y

transmita al menos los detalles de la cuenta a un dispositivo informático remoto que concede acceso al entorno de acceso controlado.

10. El método de cualquiera de las reivindicaciones 1 a 9 anteriores, en el que la notificación de autorización incluye al menos uno de:

una contraseña;

el identificador de usuario;

el identificador del dispositivo móvil;

la solicitud de transacción;

la información de control de acceso;

información sobre al menos una cuenta de transacción;

información que indica que el usuario ha sido autorizado para acceder al entorno de acceso controlado (100); e

información que indica que el usuario ha sido autenticado de manera biométrica.

11. El método de cualquiera de las reivindicaciones 1 a 10 anteriores, en el que el entorno de acceso controlado (100) incluye uno o más de:

una ubicación física;

uno o más dispositivos informáticos;

un dispositivo de almacenamiento de ordenador;

una base de datos; y

un dispositivo electrónico.

12. Un sistema para autorizar el acceso a un entorno de acceso controlado (100), comprendiendo el sistema:

una interfaz de comunicación de red (250);

un medio de almacenamiento legible por ordenador (290);

uno o más procesadores (210), configurados para interactuar con la interfaz de comunicación de red y el medio de almacenamiento legible por ordenador y ejecutar uno o más módulos de software (130) almacenados en el medio de almacenamiento, que incluye:

un módulo de base de datos (178) que, cuando es ejecutado, configura uno o más procesadores (210) para acceder a una o más bases de datos de perfiles de usuario, incluyendo los perfiles de usuario claves respectivas que identifican de manera única a los usuarios (124) respectivos emparejados con los dispositivos móviles (101a) respectivos, y las cuentas de transacción respectivas que están asociadas con los entornos de acceso controlado respectivos;

un módulo de inscripción, que cuando es ejecutado por el procesador, configura uno o más procesadores para inscribir una pluralidad de usuarios, en el que, para cada uno de la pluralidad de usuarios, la inscripción incluye:

recibir, desde un dispositivo móvil respectivo, una aplicación de capa de puertos seguros SSL de dos direcciones, un certificado y una interfaz de programación de aplicaciones, API, una clave que identifica de manera única una aplicación de autenticación biométrica concreta que se ejecuta en el dispositivo móvil respectivo, en el que el dispositivo móvil respectivo es el dispositivo informático, móvil, personal, de un usuario respectivo,

establecimiento, por el dispositivo informático, de una sesión de comunicación segura inicial con el dispositivo móvil respectivo en base al certificado de SSL bidireccional de la aplicación recibida,

recepción, por el dispositivo informático del dispositivo móvil respectivo durante la sesión de comunicación segura inicial, de información de identificación asociada con el usuario respectivo y el dispositivo móvil respectivo, y

en el que el módulo de inscripción configura, además, el procesador para, durante la sesión inicial de

comunicación segura, provocar la asignación de la clave respectiva, en el que la clave respectiva es una capa de puertos seguros, SSL, de dos direcciones cifrada, una clave asignada en base a la confirmación de la información de identificación asociada con el usuario respectivo y el dispositivo móvil respectivo durante la inscripción del usuario respectivo, y en el que se proporciona una clave privada respectiva que corresponde a la clave respectiva en el dispositivo móvil respectivo y es almacenada por el dispositivo móvil respectivo durante la inscripción, en el que la clave privada respectiva es una clave de SSL de dos direcciones, cifrada, que es adecuada para identificar de manera exclusiva al usuario respectivo emparejado con el dispositivo móvil respectivo y establecer sesiones de comunicación seguras posteriores entre el dispositivo móvil respectivo y el dispositivo informático;

un módulo de comunicación (182) que, cuando es ejecutado configura uno o más procesadores (210) para recibir información de control de acceso que identifica el entorno de acceso controlado y para recibir desde un dispositivo móvil a través de una red, una solicitud de transacción que comprende uno o más transmisiones, e incluye: a) una clave privada respectiva, en la que la clave privada respectiva es adecuada para identificar a un usuario emparejado con el dispositivo móvil, y b) una indicación de si el dispositivo móvil ha autenticado al usuario en base a los datos biométricos del usuario:

un módulo de autorización (180) que, cuando es ejecutado, configura uno o más procesadores (210) para procesar, utilizando al menos una base de datos (280), la solicitud de transacción para autorizar al usuario a acceder al entorno de acceso controlado mediante:

verificación de que la clave privada respectiva recibida corresponde a una clave respectiva almacenada en un perfil de usuario y, según la verificación, establecimiento de una sesión de comunicación cifrada entre el dispositivo móvil y el dispositivo informático utilizando la clave privada respectiva,

verificación de que la indicación confirma que la identidad del usuario ha sido autenticada por el dispositivo móvil en base a los datos biométricos del usuario,

verificación de que una o más transmisiones se ajustan a una configuración predeterminada, y

determinación de que el perfil de usuario correspondiente a la clave privada respectiva identifica una cuenta de transacción que está asociada con el entorno de acceso controlado;

en el que el módulo de autorización (180) también configura uno o más procesadores (210) para generar una notificación de autorización que facilita al usuario autorizado acceder al entorno de acceso controlado (100); y

en el que el módulo de comunicación (182) configura, además, el uno o más procesadores (210) para transmitir la notificación de autorización a al menos un dispositivo informático remoto a través de una red.

13. El sistema de la reivindicación 12, en el que la solicitud de transacción comprende una pluralidad de transmisiones, y en el que el módulo de autorización (180) configura el procesador para verificar que la clave privada respectiva corresponde a la clave respectiva: determinando que la clave privada respectiva proporcionada en cada de la pluralidad de transmisiones corresponde a la clave respectiva almacenada en el perfil del usuario.

14. El sistema de cualquiera de las reivindicaciones 12 a 13 anteriores, en el que la información de control de acceso identifica adicionalmente al usuario, en el que el módulo de autorización (180) configura, adicionalmente, el uno o más procesadores para:

procesar la información de control de acceso para identificar en la base de datos un perfil de usuario que identifique al usuario, e identificar el dispositivo móvil en el perfil de usuario;

generar una solicitud de autenticación biométrica que facilite la autenticación biométrica del usuario; y

transmitir al dispositivo móvil (101a) a través de la red, la solicitud de autenticación biométrica para que el dispositivo móvil autentique de manera biométrica al usuario (124).

15. El sistema de cualquiera de las reivindicaciones 12 a 14 anteriores, en el que el perfil del usuario incluye información de la cuenta de transacción relacionada con la cuenta de la transacción, y en el que la al menos una base de datos (280) incluye al menos una regla de acceso que restringe el acceso al entorno de acceso controlado (100); y en el que el módulo de autorización (180) configura adicionalmente el uno o más procesadores (210) para:

recuperar la al menos una regla de acceso de la al menos una base de datos (280) en base, al menos, a la información de control de acceso;

recuperar la información de la cuenta de transacción del perfil de usuario; y

además, autorizar al usuario a acceder al entorno de acceso controlado (100) en base a la información de la cuenta de la transacción y a la al menos una regla de acceso.

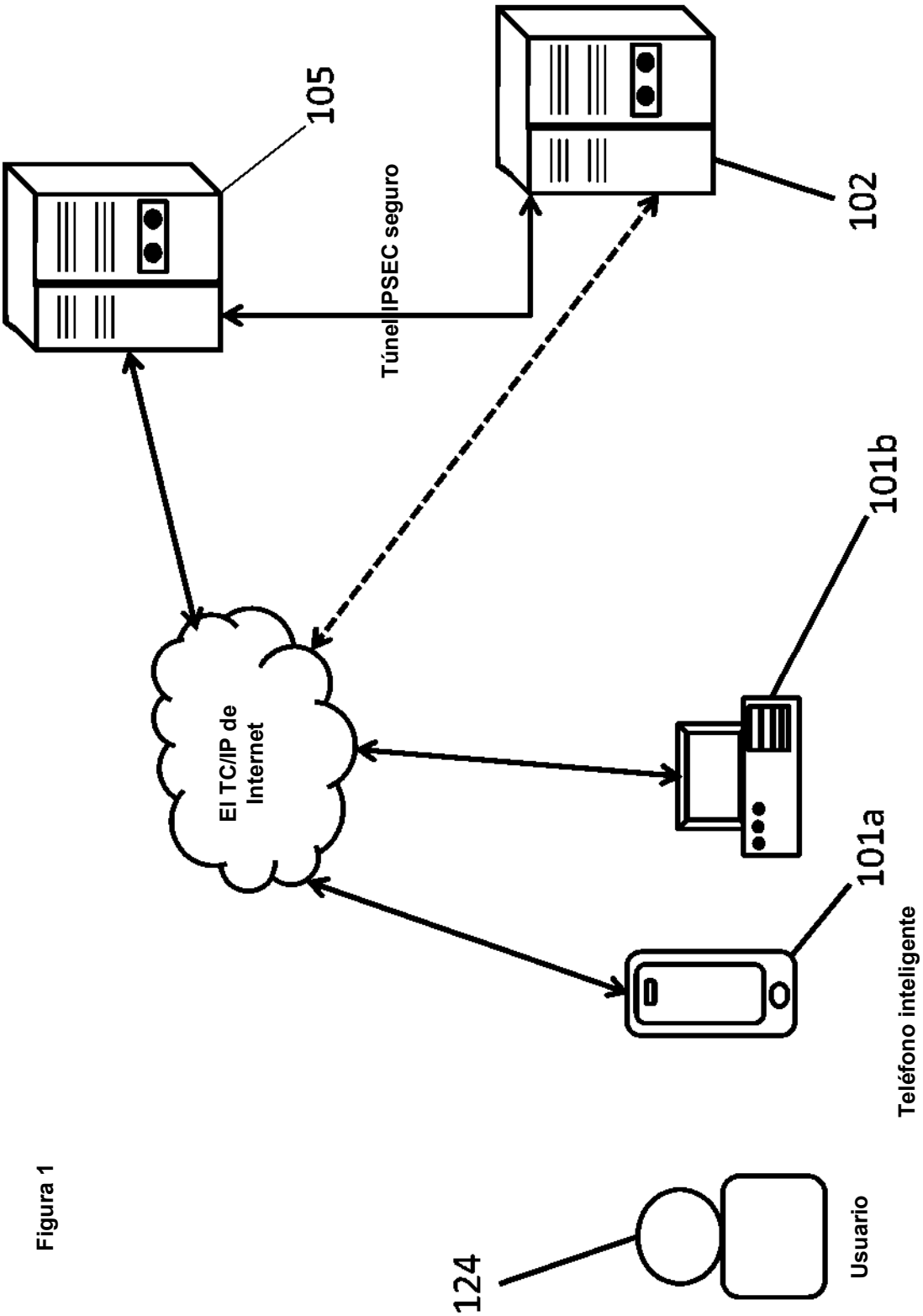
105
102
Túnel IPSEC seguro
El TC/IP de Internet
101b
101a
Teléfono inteligente
124
Usuario

Figura 1

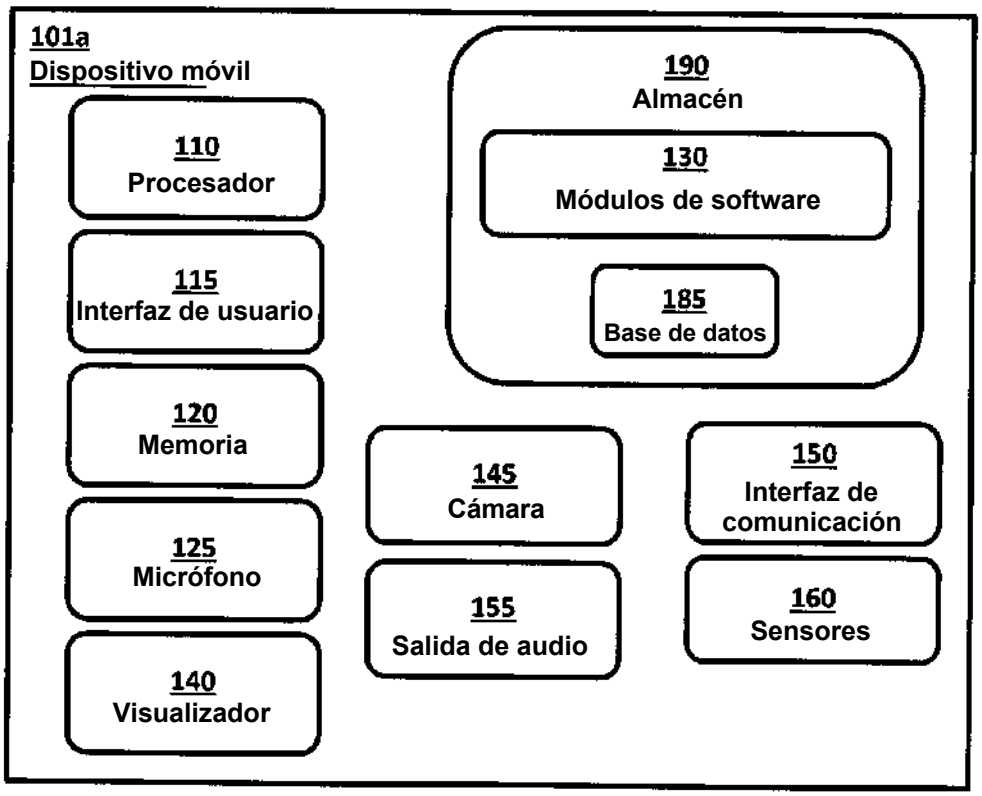
101a
Dispositivo móvil
110
Procesador
115
Interfaz de usuario
120
Memoria
125
Micrófono
140
Visualizador
190
Almacén
130
Módulos de software
185
Base de datos
145
Cámara
155
Salida de audio
150
Interfaz de comunicación
160
Sensores

Figura 2A

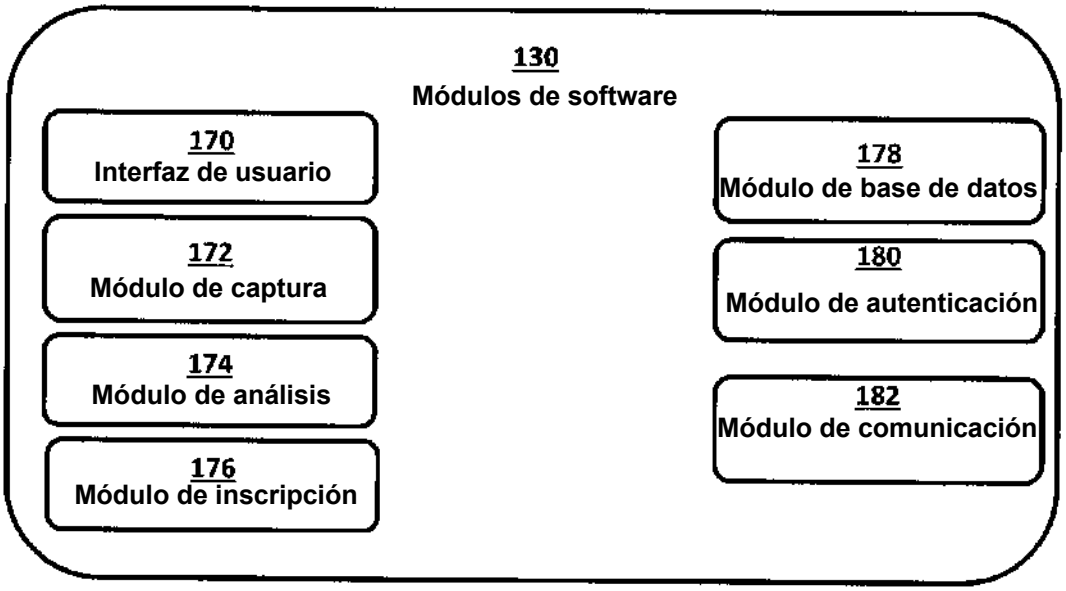

Figura 2B

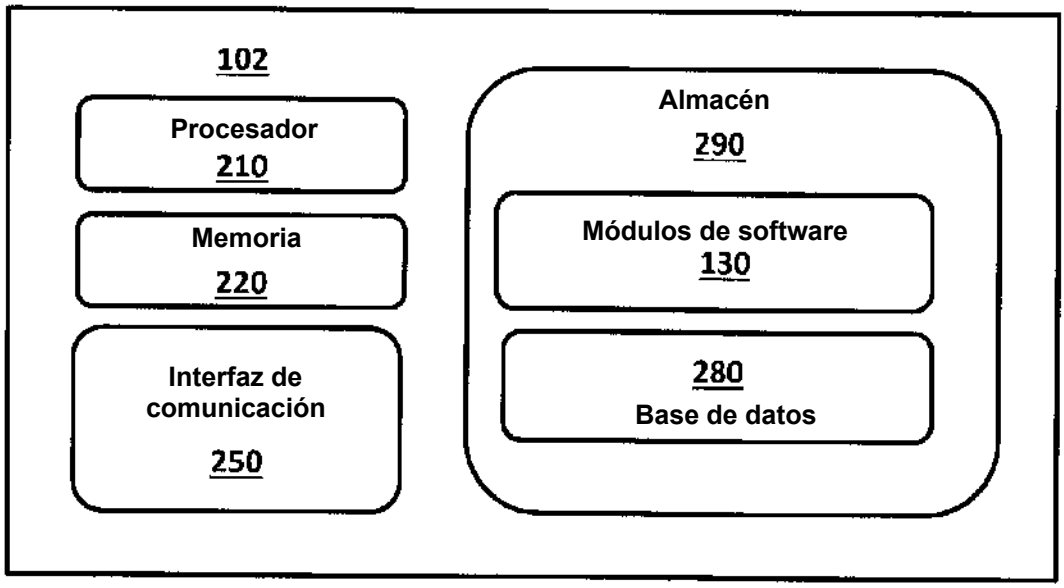

Figura 2C

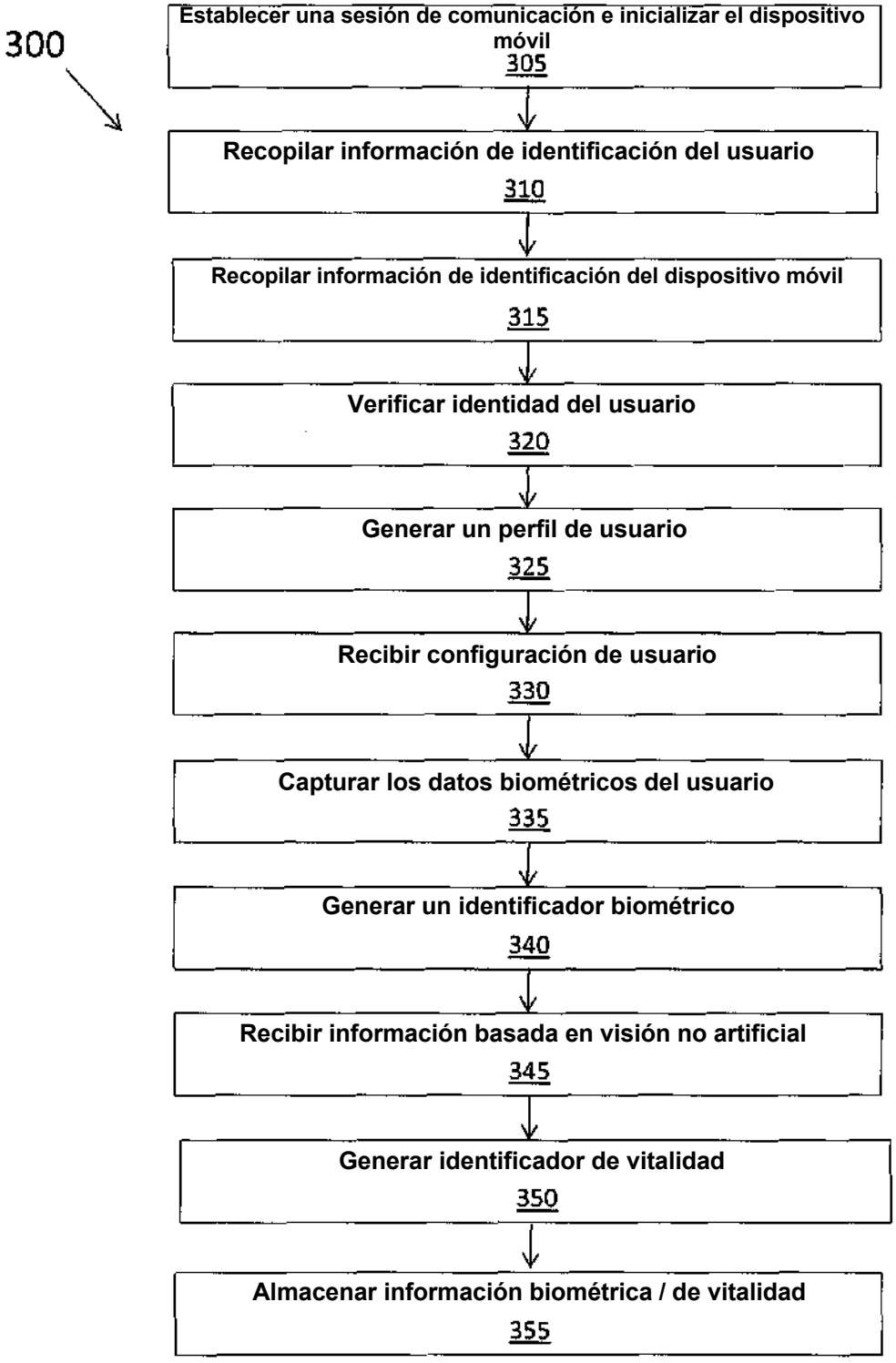
300
Establecer una sesión de comunicación e inicializar el dispositivo móvil
305
Recopilar información de identificación del usuario
310
Recopilar información de identificación del dispositivo móvil
315
Verificar identidad del usuario
320
Generar un perfil de usuario
325
Recibir configuración de usuario
330
Capturar los datos biométricos del usuario
335
Generar un identificador biométrico
340
Recibir información basada en visión no artificial
345
Generar identificador de vitalidad
350
Almacenar información biométrica / de vitalidad
355

Figura 3

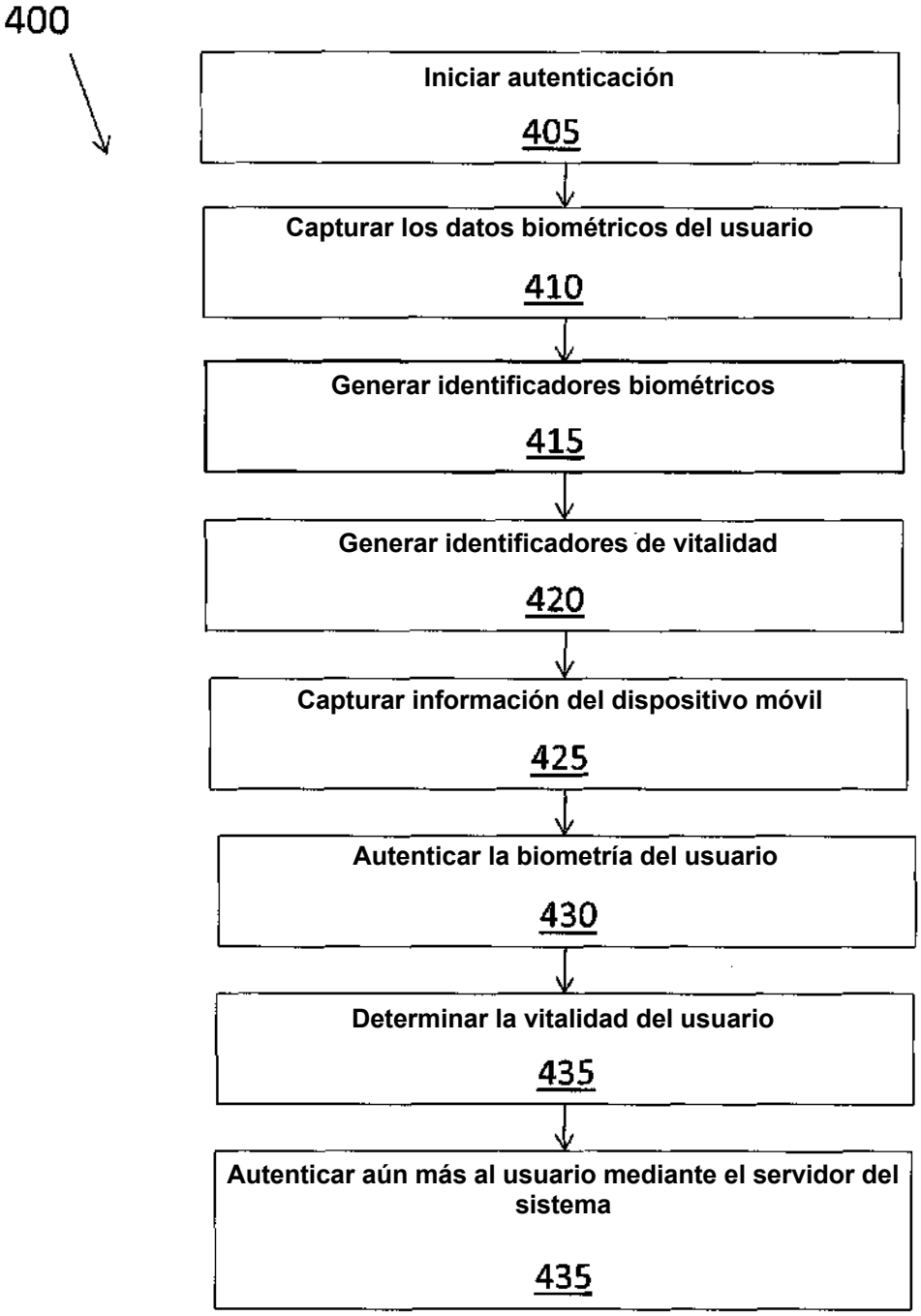
400
Iniciar autenticación
405
Capturar los datos biométricos del usuario
410
Generar identificadores biométricos
415
Generar identificadores de vitalidad
420
Capturar información del dispositivo móvil
425
Autenticar la biometría del usuario
430
Determinar la vitalidad del usuario
435
Autenticar aún más al usuario mediante el servidor del sistema
435

Figura 4

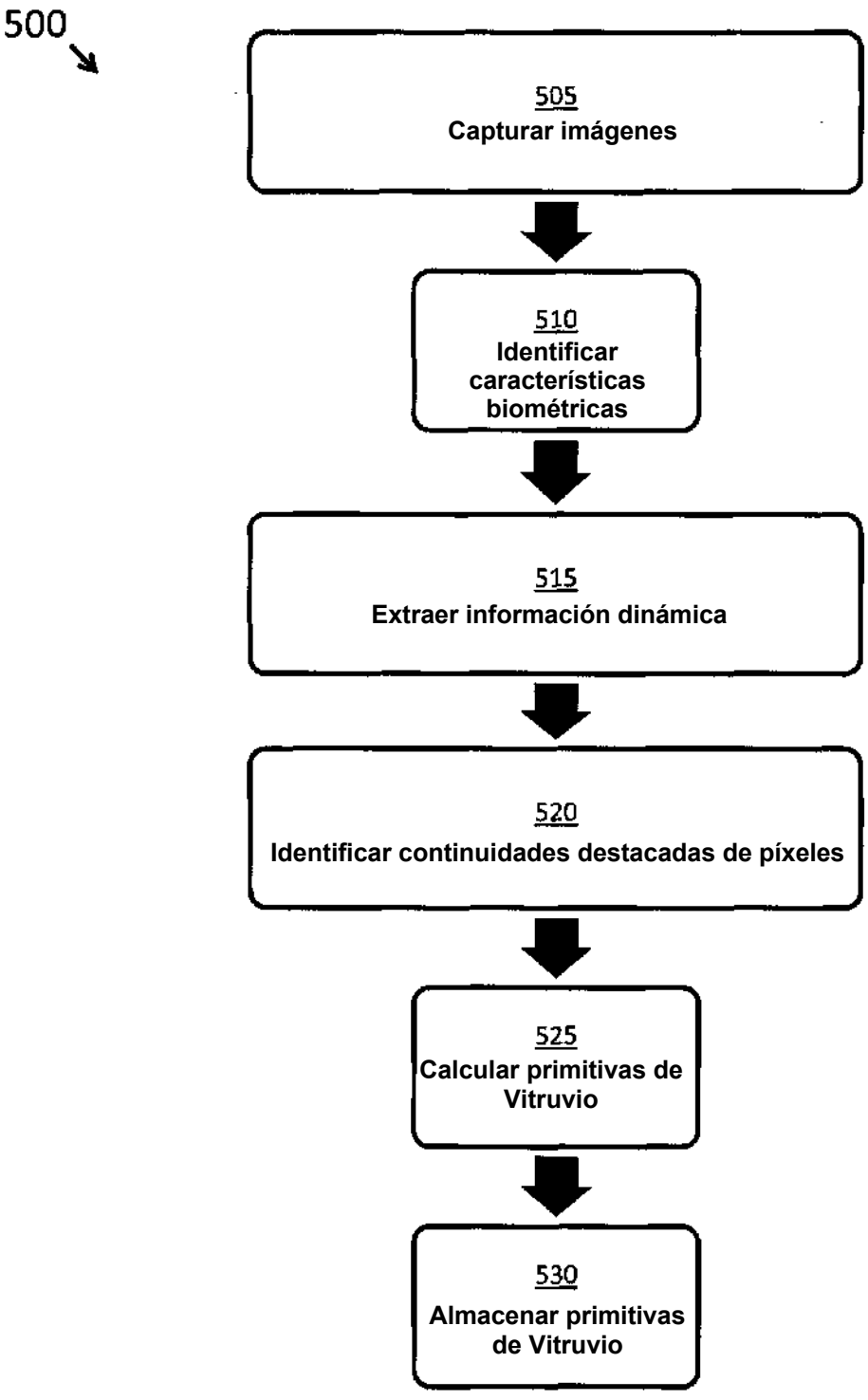
500
505
Capturar imágenes
510
Identificar características biométricas
515
Extraer información dinámica
520
Identificar continuidades destacadas de píxeles
525
Calcular primitivas de Vitruvio
530
Almacenar primitivas de Vitruvio

Figura 5

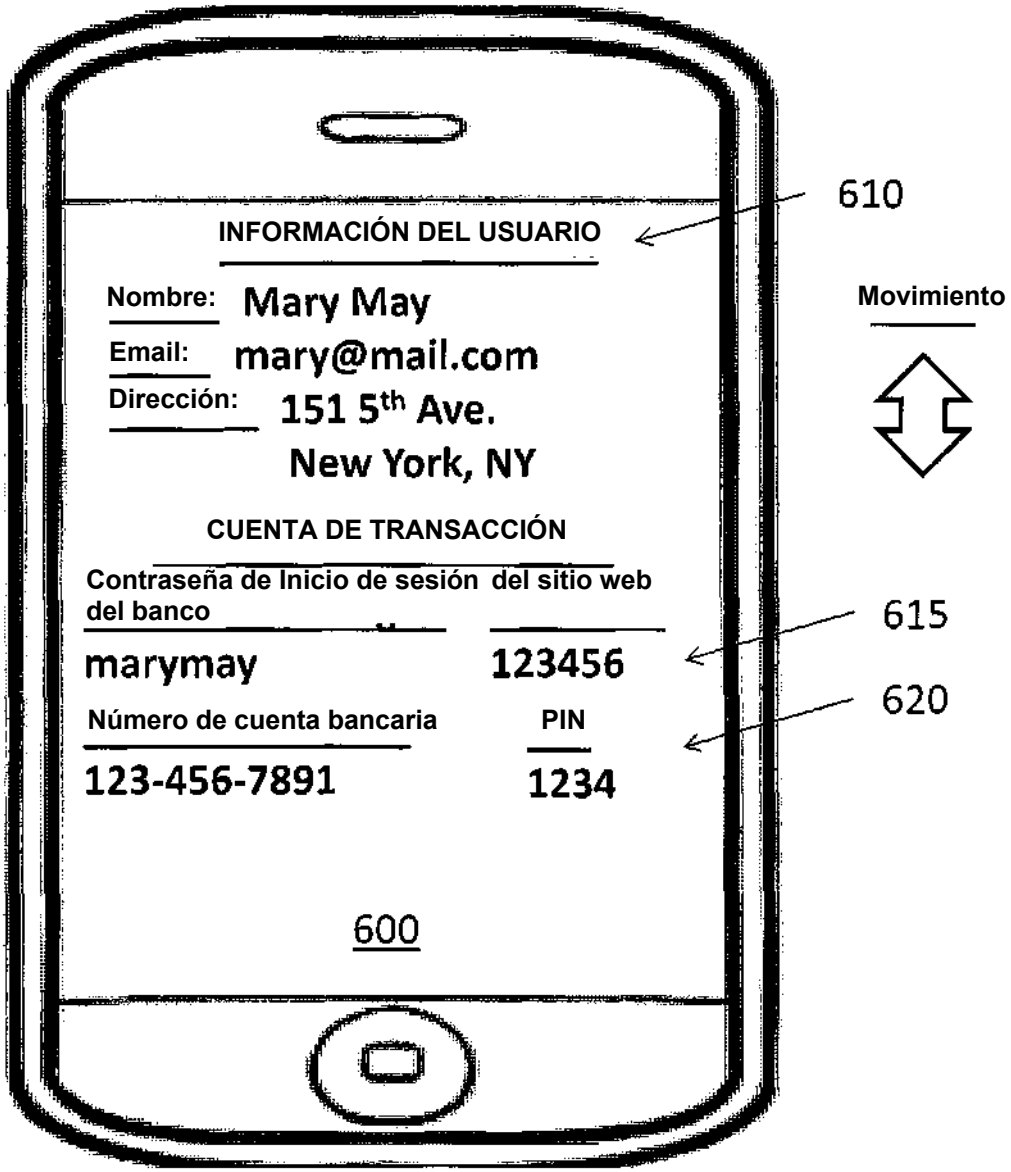
610
INFORMACIÓN DEL USUARIO
Nombre: Mary May
Email: mary@mail.com
Dirección: 151 5th Ave.
New York, NY
CUENTA DE TRANSACCIÓN
Contraseña de Inicio de sesión del sitio web del banco
marymay
123456
615
Número de cuenta bancaria
123-456-7891
PIN
1234
620
600
Movimiento

Figura 6A

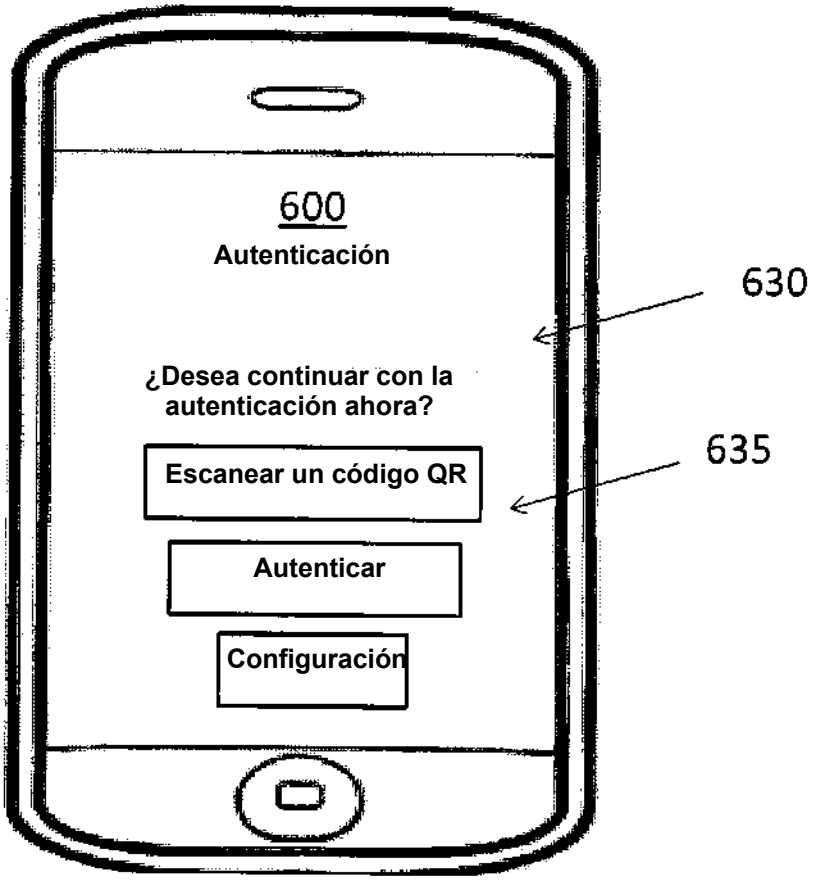
600
Autenticación
630
¿Desea continuar con la autenticación ahora?
635
Escanear un código QR
Autenticar
Configuración

Figura 6B

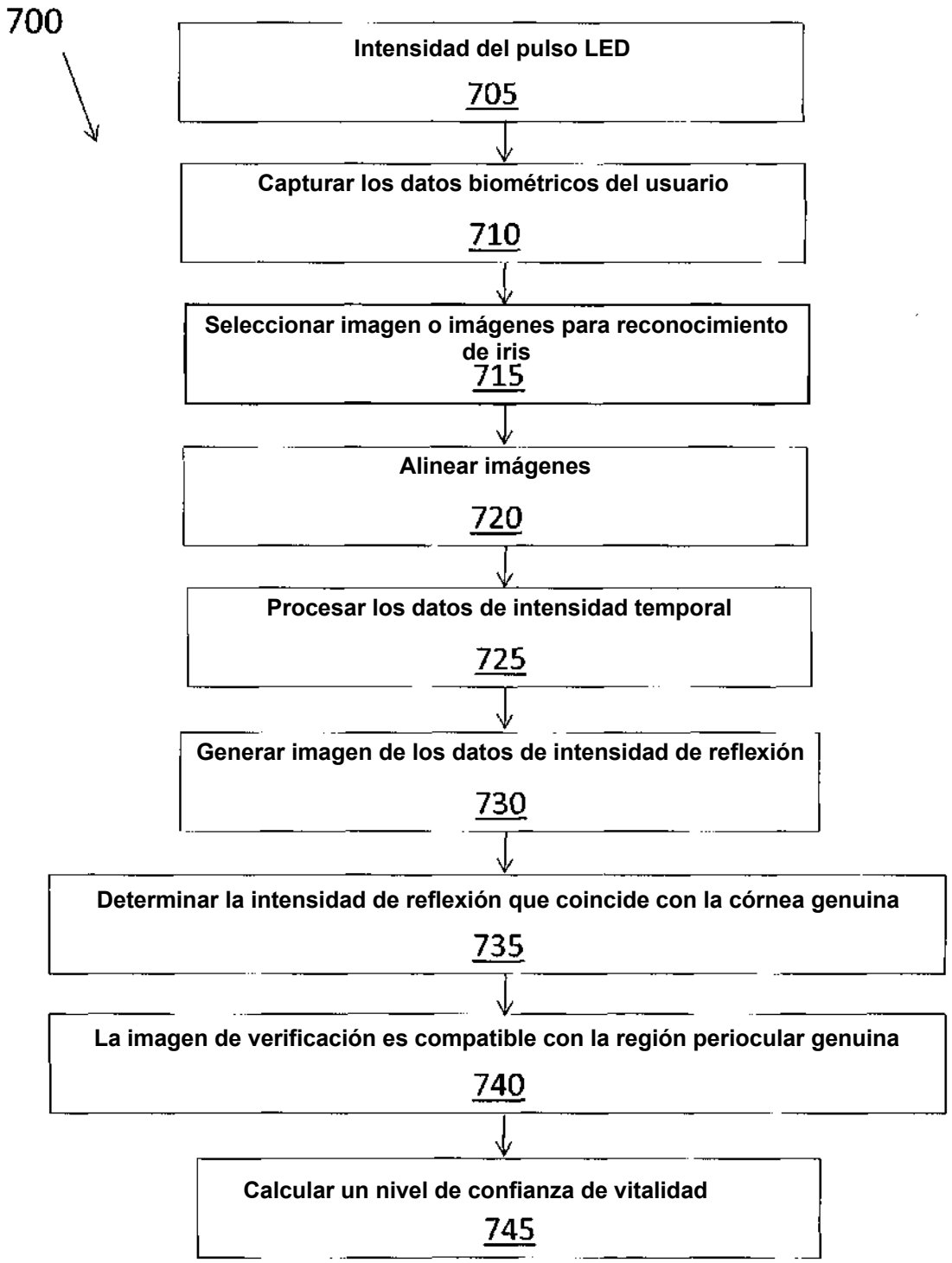
700
Intensidad del pulso LED
705
Capturar los datos biométricos del usuario
710
Seleccionar imagen o imágenes para reconocimiento de iris
715
Alinear imágenes
720
Procesar los datos de intensidad temporal
725
Generar imagen de los datos de intensidad de reflexión
730
Determinar la intensidad de reflexión que coincide con la córnea genuina
735
La imagen de verificación es compatible con la región periocular genuina
740
Calcular un nivel de confianza de vitalidad
745

Figura 7