(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 645 975**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/32 (2013.01)
H04L 9/32 (2006.01)
G06K 9/00 (2006.01)
G06Q 20/40 (2012.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **04.06.2013 PCT/EP2013/061521**

(87) Fecha y número de publicación internacional: **11.12.2014 WO14194939**

(96) Fecha de presentación y número de la solicitud europea: **04.06.2013 E 13730502 (5)**

(97) Fecha y número de publicación de la concesión europea: **09.08.2017 EP 3005639**

(54) Título: **Método y sistema para verificar la identidad de un usuario de un servicio en línea**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2017

(73) Titular/es:

SMILEY OWL TECH S.L. (100.0%)
Arturo Campion 22
20018 Donostia (San Sebastián), Gipuzkoa, ES

(72) Inventor/es:

VEA ORTE, RICARDO;
LABAYEN ESNAOLA, MIKEL;
FLOREZ ESNAL, JULIÁN y
MARCOS ORTEGO, GORKA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y sistema para verificar la identidad de un usuario de un servicio en línea.

Campo técnico

La presente invención se refiere al campo de acceso seguro a los servicios de Internet y la verificación continua durante las sesiones activas y, en particular, a métodos y sistemas para evitar el robo de identidad en servicios en línea.

Estado de la técnica

Hoy en día, la identificación de usuarios en servicios en línea o servicios web está vinculada a una asignación previa de usuario y contraseña. Esta información puede, con o sin el consentimiento del usuario, establecer el robo de identidad, ya que la contraseña se puede compartir, robar o perder.

Existen aplicaciones bien conocidas que utilizan el reconocimiento facial con diferentes propósitos. A continuación, se presentan ejemplos de estas aplicaciones.

Algunas empresas que se ocupan de las aplicaciones en la nube utilizan técnicas de reconocimiento facial para fines de gestión y etiquetado. Ejemplos de tecnologías de reconocimiento de imágenes son *Neven Vision* desarrolladas por Nevenengineering, Inc. y compradas por Google, *face.com* compradas por Apple o *Polar Rose* compradas por Flickr y Facebook. También existen bibliotecas gratuitas, como *Fotobounce,* para el reconocimiento facial para la gestión y etiquetado de fotos. Estas aplicaciones web usan técnicas de reconocimiento facial como herramientas para el etiquetado automático de fotos. Las caras se identifican y las imágenes de las personas que aparecen etiquetadas. Estas plataformas generalmente ofrecen servicios de valor agregado, como recomendar nuevos contactos, vincular amigos comunes, agrupar imágenes, etc.

Probablemente, la aplicabilidad más amplia de las técnicas de reconocimiento facial se puede encontrar en el mundo de la seguridad. Tanto las instituciones de seguridad privadas como públicas utilizan estas técnicas para identificar a las personas que pueden implicar un peligro. Una imagen facial, tomada por sensores ubicados en edificios o incluso ciudades, generalmente se compara con una gran cantidad de imágenes almacenadas en bases de datos de personas potencialmente peligrosas. Los productos que proporcionan esta posibilidad de compatibilidad son, por ejemplo, Congnitec, que proporciona coincidencia de fotografías en grandes bases de datos, Smartmatic, Face first, aware, Inc. o Morphotrak. Todos ofrecen soluciones independientes sin conexión.

Finalmente, existen soluciones comerciales que tienen como objetivo el control de acceso en áreas físicas o edificios. Ejemplos de tales soluciones son Justlook o Synel's. Estas aplicaciones están instaladas en los terminales de acceso. Por medio de una base de datos propiedad de la misma entidad, verifican la identidad de la persona que intenta ingresar, dando o denegando dicho acceso físico. También existen sistemas basados en reconocimiento facial, como KeyLemon, para verificar el acceso al equipo. Esta solución controla el establecimiento de sesión en un ordenador por medio de reconocimiento facial en lugar de requerir una ID y una contraseña de usuario. Se instala localmente en el ordenador y se ejecuta sin conexión. De manera similar, el sistema operativo Android 4.0 incluye una aplicación de reconocimiento facial que, en principio, es válida para desbloquear terminales móviles.

La solicitud de patente US2012/0106805A1 divulga un método para la verificación de identidad en línea.

La Patente de los Estados Unidos US7991388B1 divulga un método y un sistema para autenticar un titular de cuenta. El método y el sistema implican que el usuario se fotografíe a sí mismo para la verificación del reconocimiento facial, la determinación de la ubicación geográfica y el tecleado del PIN.

Sin embargo, ninguna de las solicitudes mencionadas trata el problema de garantizar el acceso seguro a los servicios web o el uso continuo y seguro de sesiones completas de servicios web. Por el contrario, son programas independientes que se ejecutan localmente en el terminal en la que están instalados y solo abordan el problema de garantizar un acceso seguro.

Assad Moini y Azad M. Madni debaten en "Leveraging Biometrics for User Authentication in Online Learning: A System Perspective", IEEE Systems Journal, Vol. 3, n.º 4, diciembre de 2009, biometría para la autenticación remota en el aprendizaje en línea, incluida la autenticación continua.

En resumen, existe la necesidad de resolver de manera eficiente, el problema del robo de identidad cuando se accede a servicios web o cuando se utilizan de manera continua sesiones de servicios web.

Descripción de la invención

Es un objetivo de la presente invención proporcionar un método de un sistema y un producto de programa informático, para un acceso seguro a los servicios web y un uso continuo y seguro de las sesiones de servicios web como se describe en las reivindicaciones adjuntas. Las ventajas y características adicionales de la invención se harán evidentes a partir de la descripción detallada que sigue y se señalará particularmente en las reivindicaciones adjuntas.

Breve descripción de los dibujos

Para completar la descripción y para proporcionar una mejor comprensión de la invención, se proporciona un conjunto de dibujos. Dichos dibujos forman parte integrante de la descripción e ilustran una realización de la invención, que no debe interpretarse como que restringe el alcance de la invención, sino simplemente como un ejemplo de cómo se puede llevar a cabo la invención. Los dibujos comprenden la siguiente figura:

La figura 1 es un flujo de trabajo del método de acuerdo con una posible realización de la presente invención.

Descripción de una manera de llevar a cabo la invención

El método y el sistema de la invención representan un servicio de valor agregado dirigido a entidades que ofrecen servicios en línea y requieren autenticación de usuario. El método proporciona una solución al robo de identidad en el mundo en línea, ya que proporciona una verificación continua de la identidad de las personas que utilizan un servicio web. Dicha verificación se basa en el reconocimiento facial y se consigue tomando repetidas imágenes del usuario con una cámara web y comparando esas imágenes con la información almacenada del usuario suscrito. El método se explica en detalle a continuación.

En el contexto de la presente invención, los términos "dibujo", "imagen" y "foto" se usan indistintamente. Lo mismo se aplica a las expresiones "servicio web" y "servicio en línea", que también se refieren a servicios remotos cuyo acceso requiere una conexión a Internet.

También en el contexto de la presente invención, el término "continuo", referido a "validación continua" o "verificación continua" de una sesión (de un servicio en línea), significa que la identidad del usuario que está utilizando dicha sesión se verifica no solo en el momento de dar acceso (para iniciar la sesión) al usuario, sino también en varios momentos diferentes durante la vida de la sesión activa. Esta verificación puede ser periódica (con la periodicidad que el proveedor del servicio decide imponer) o aleatoria (con la ventaja de sorprender al usuario). En otras palabras, "muestras" (en este caso, fotos) del usuario se toman en momentos discretos durante la sesión para verificar continuamente su identidad.

La figura 1 es un flujo de trabajo del método para verificar la identidad de los usuarios de un servicio web. En la figura 1, se muestran esquemáticamente un terminal de usuario 1, un servicio web 2 y un tercero o tercera entidad 20. El tercero 20 es el proveedor del servicio de autenticación de la invención.

El terminal de usuario 1 es el terminal utilizado por un usuario final para acceder a un servicio en línea administrado por un proveedor de servicios. Ejemplos no limitantes de terminales de usuario 1 son ordenadores personales, ordenadores portátiles, terminales celulares o móviles o cualquier otro terminal a través del cual se pueda establecer una conexión de datos. Se puede usar cualquier terminal, siempre que se pueda establecer una conexión de datos. Y se puede usar cualquier navegador convencional dentro de dicho terminal. El método inventivo no impone ningún requisito de software en este terminal de usuario 1 que vaya más allá de los requisitos mínimos para acceder al servicio web. Esto significa que el terminal de usuario 1 no necesita ningún complemento o componente de software instalado. El terminal de usuario 1 tiene una cámara web que debe estar habilitada.

El bloque 2 en la figura 1 representa un servicio en línea (también conocido como servicio web) ofrecido por un proveedor de servicios. En particular, este bloque comprende tanto el servidor o servidores y el sitio web correspondiente para proporcionar un servicio en línea ofrecido por un proveedor de servicios. Para que un usuario acceda desde un terminal de usuario 1 al servicio en línea ofrecido por el proveedor, el usuario debe visitar un sitio web 2 del proveedor. El servidor contiene, entre otras cosas, una orden para ejecutar una aplicación de control del tercero (preferiblemente ejecutada en la nube) e información de la ubicación desde donde los terminales de usuario 1 deben descargar aplicaciones para el registro de usuarios y posterior verificación mediante captura de fotografías. Preferiblemente, la información de ubicación es una dirección IP de un servidor 3 de un tercero 20 que proporciona el servicio de verificación y autenticación. Preferiblemente, los servidores y las bases de datos de este tercero se encuentran en la nube.

En una realización particular, el servicio ofrecido por el proveedor del servicio es un servicio educativo en el que los usuarios siguen un curso o capacitación en línea, para lo cual su identidad debe ser frecuentemente revisada si ellos (estudiantes) desean obtener un título. Ejemplos no limitantes de otros servicios en línea o servicios web que también pueden proporcionar el proveedor de servicios son, entre otros: pago electrónico, acceso en línea a cuentas

bancarias, juegos en línea y monitorización.

La comunicación entre el usuario (en el terminal de usuario 1) y el proveedor de servicios web (a través del sitio web 2) para recibir o usar el servicio en línea es la siguiente (etapa A en la figura 1): Un usuario final (por ejemplo, un estudiante que quiere seguir un curso en línea) visita (flecha A1) utilizando una terminal de usuario 1 una página web desde la cual el proveedor ofrece su servicio en línea 2. Esta conexión se establece a través de cualquier protocolo convencional de comunicaciones de datos. En una realización preferida, esta comunicación se establece utilizando el protocolo de Internet. El usuario descarga (flecha A2) la página web y/o el servicio en línea desde los servidores del proveedor 2. En una realización preferida, el usuario descarga (A2) una página web que actúa como interfaz de usuario. En otras palabras, se descarga la página web del servicio y, a través de la interacción con dicha página web, un sitio vinculado a la página web ofrece su servicio en línea (por ejemplo, servicio de archivos, ejercicios en línea, foros ...).

El proveedor de servicios ha integrado dentro de su servidor 2: (a) información (por ejemplo, una dirección IP) para descargar aplicaciones de terceros y (b) una orden para ejecutar una aplicación de control 30 desde el servidor de aplicaciones 3 del tercero 20 (o, mejor dicho, desde la nube, donde el servidor de aplicaciones 3 conserva su información). El proveedor de servicios también tiene datos que identifican inequívocamente al usuario que está conectado a un servicio web, ya que obtiene esta información cuando el usuario se conecta al servicio en línea a través de una página web (que requiere iniciar sesión con la ID y contraseña del usuario).

Junto con la página web descargada (flecha A2), el terminal de usuario 1 recibe (descarga) esa orden para ejecutar dicha aplicación de control 30 perteneciente a un módulo de aplicaciones o servidor de aplicaciones 3. Dentro de este orden, también hay algunos datos que identifican inequívocamente al usuario que ha iniciado sesión en el servicio en línea 2 (por ejemplo, una ID de usuario). El terminal de usuario 1 también recibe (flecha A2) junto con o dentro de dicho orden de ejecución una dirección IP del módulo de aplicaciones 3 del tercero 20. La aplicación de control 30 se mantiene preferiblemente en la nube. Esta aplicación de control 30 controla la descarga de aplicaciones de terceros adicionales (es decir, aplicaciones ofrecidas por un tercero 20) de un módulo de aplicaciones o servidor de aplicaciones 3 (también denominado servidor de autenticación 3), que son la clave para registro de usuario y ulterior (ya sea de manera periódica o no periódica) del usuario. Preferiblemente, esas aplicaciones se mantienen en la nube. En otras palabras, el terminal de usuario 1 recibe (flecha A2) la dirección IP en la que puede ejecutar una aplicación de control remota 30 y en la que puede descargar las aplicaciones de terceros, y un pedido para ejecutar la aplicación de control remota 30, y datos que identifican inequívocamente al usuario que ha iniciado sesión en el servicio en línea 2.

De este modo, cada usuario que accede al servicio en línea 2 recibe (A2) el orden de ejecución de esa aplicación de control, la información (dirección IP) para llegar al servidor de aplicaciones 3 y la identificación del usuario del servicio web 2. Sin embargo, puede suceder que el proveedor del servicio no esté interesado, por ningún motivo, en controlar a todos los usuarios de su servicio en línea. Por lo tanto, es el proveedor del servicio el que autoriza o niega la autorización a los usuarios para descargar esas aplicaciones adicionales del tercero (servidor 3). Si el proveedor de servicios decide no autorizar a un usuario a utilizar el servicio de verificación provisto por el tercero 20, la sesión en línea con el servicio en línea 2 se ejecuta de manera convencional (es decir, sin verificación continua de la identidad del usuario).

La *inteligencia* del tercero 20 reside principalmente en un módulo de gestión 4, a cargo, entre otras tareas, de gestionar el acceso de imágenes (entrada y salida) a una base de datos 5; administrar el flujo de trabajo entre los módulos de reconocimiento facial automáticos y manuales, en función de la precisión de los resultados de reconocimiento facial automático entregados; y la gestión de la entrega de imágenes validadas manualmente a un entrenador facial para la actualización continua de los modelos faciales de los usuarios.

El tercero 20 también tiene una base de datos 5 para almacenar todas las imágenes capturadas, metadatos asociados y modelos biométricos de caras de usuario.

Una vez que el terminal de usuario 1 ha recibido (flecha A2) la orden de ejecución para ejecutar una aplicación de control 30, el terminal de usuario 1 ordena (flecha B1) la ejecución de una aplicación de control 30 que pertenece al servidor 3 del tercero y preferiblemente se mantiene en la nube. A continuación, se ejecuta una aplicación de control 30 preferentemente en la nube. Luego esta aplicación de control 30 verifica si al usuario en el terminal 1 de usuario que intenta acceder a una sesión (del servicio web) controlado por la autenticación facial proporcionada por el tercero 20, se le permite acceder a dicha sesión o no. Esta aplicación 30 verifica si el usuario está autorizado o no por el proveedor del servicio. Como ya se explicó, es posible que el proveedor de servicios no esté interesado en controlar a todos los usuarios de su servicio en línea. Por lo tanto, se deniega la autorización para descargar las aplicaciones de verificación a los usuarios no autorizados. Finalmente, si un usuario está autorizado, la aplicación 30 verifica si él o ella ya está registrado o no.

A continuación, se explica cómo se verifica si un usuario está autorizado a utilizar un servicio de verificación facial o no. Una vez que se ejecuta la aplicación de control 30, el servidor de aplicaciones 3 proporciona algunos datos que identifican inequívocamente al usuario que intenta establecer la sesión. En una realización preferida, esos datos son

una ID de usuario. Estos datos se obtuvieron previamente (flecha A2) del proveedor del servicio, ya que esos datos se incluyeron en la orden de ejecución enviada al terminal de usuario 1 (flecha A2). El servidor de aplicaciones (servidor de autenticación) 3 hace una petición (flecha C1) a un módulo de gestión 4 propiedad del tercero 20, que comprueba (flecha E1) en una base de datos 5 si los datos identifican inequívocamente al usuario (preferiblemente un usuario ID) corresponden a un usuario que está autorizado para usar una sesión controlada de reconocimiento facial o no. Si el usuario no está permitido, el módulo de gestión 4 (flecha C2) informa al servidor de aplicaciones 3 y se interrumpe la ejecución de la aplicación 30 y se informa al terminal de usuario 1 (flecha B2) de esta interrupción. Las aplicaciones adicionales (31, 32, 33) no se descargan. La comunicación entre el usuario (en el terminal de usuario 1) y el servicio web/servidores 2 sigue como una conexión cliente/servidor convencional (sin usar el método para la verificación continua de identidad). Como ya se explicó, es el proveedor de servicios en línea el que autoriza (o no) a los usuarios en el servicio de terceros para la verificación de identidad.

Solo cuando un usuario es autorizado por el proveedor de servicios del servicio en línea 2, comienza una sesión controlada por el tercero 20 (este inicio está controlado por la aplicación de control 30). En esta sesión controlada se toman fotos y la identidad de las personas que aparecen en esas fotos se verifica mediante algoritmos de autenticación facial, como se explica a continuación.

El servidor de aplicaciones (servidor de autenticación) 3 mantiene al menos tres aplicaciones adicionales: una solicitud de registro 31, una aplicación de toma de imágenes 33 y una aplicación 32 configurada para definir las preferencias de opciones de interacción entre la aplicación de toma de imágenes 33 y el terminal de usuario 1 Las aplicaciones de terceros son compatibles con cualquier navegador. Es la aplicación de control 30 la que ordena la descarga de estas aplicaciones 31, 32, 33 en el terminal de usuario 1. El usuario necesita estas aplicaciones porque permiten que el terminal 1 del usuario establezca una conexión con una sesión controlada de reconocimiento facial ofrecida por el tercero 20. Las aplicaciones de terceros son compatibles con cualquier navegador. La aplicación de registro 31 está configurada para tomar al menos una primera imagen que se usa para el primer entrenamiento (para tener una referencia del aspecto real del usuario). La aplicación de toma de imágenes 33 es una aplicación para acceder a la cámara web del terminal de usuario 1 para la verificación de identidad del usuario. Pide a la cámara web que tome una fotografía y la envíe a un módulo de gestión 4. La aplicación 32 de preferencias está configurada para permitir que un usuario defina sus preferencias con respecto a la aplicación 33 de toma de imágenes. Estas aplicaciones 31, 32, 33 permiten el establecimiento de una sesión controlada de reconocimiento facial. Como ya se explicó, antes de establecer esta sesión controlada, la aplicación de control 30 verifica, a través del módulo de gestión 4 (que a su vez verifica en la base de datos 5), si el usuario que ha iniciado sesión en el servicio en línea 2 está habilitado para usar un reconocimiento facial sesión controlada Solo si el usuario está autorizado a utilizar la sesión controlada de reconocimiento facial, la aplicación de control 30 ordenará la descarga de esas aplicaciones 31, 32, 33 (o la requerida en un momento determinado).

Las tres aplicaciones 31, 32, 33 no se descargan en el terminal de usuario 1 al mismo tiempo. La aplicación de control 30 controla qué aplicación 31, 32, 33 debe ser descargada (flecha B2) en el terminal de usuario 1. Por ejemplo, si un usuario ya está registrado, no es necesario descargar la aplicación de registro 31 (esta aplicación 31 se descarga solo la primera vez que un usuario accede a este servicio de verificación proporcionado por el tercero 20). La aplicación de toma de imágenes 33 se descarga en todas las sesiones. La aplicación de preferencias 32 se descarga preferiblemente después de que un usuario ha sido registrado. Más tarde, esta aplicación 32 se descarga preferiblemente solo bajo demanda, cuando el usuario hace clic en una pestaña para cambiar las diferentes opciones. Por otro lado, las aplicaciones se ejecutan localmente, pero no se instala nada (se ejecutan sin estar instaladas). Son aplicaciones portátiles. Las aplicaciones se almacenan preferiblemente en la nube.

Si la tarjeta de gestión o la unidad de gestión 4 verifica (flecha E1) que se le permite al usuario (autorizado por el proveedor de servicios del servicio en línea) utilizar la sesión de control de reconocimiento facial, y el terminal de usuario 1 tiene una cámara web que es activada, el módulo de aplicaciones 3 pregunta (flecha C3) al módulo de gestión 4 si el usuario está registrado o no en el sistema (es decir, si el sistema ya tiene una imagen (una cara) del usuario en su base de datos 5). Después de verificar esta información en la base de datos 5 (flecha E2), el módulo de gestión 4 informa (flecha C4) al módulo de aplicaciones 3. Todo este flujo de trabajo de información está controlado por la aplicación de control 30. Según los resultados, el flujo de trabajo continúa de la siguiente manera:

Caso 1: El usuario no está registrado todavía

Si el usuario no está registrado todavía con el tercero 20 a cargo de verificar que se obtiene el acceso seguro al servicio web 2, la aplicación de control 30 da una orden para descargar (flecha B2) en el terminal de usuario 1 una aplicación de registro 31. Esta aplicación de registro interno 31 se basa en la tecnología Flex de Adobe y es un desarrollo patentado de los inventores de la patente.

A continuación, si un usuario está autorizado por el proveedor de servicios para utilizar el servicio de verificación ofrecido por el tercero 20, la solicitud de registro 31 comprueba si el usuario tiene, en su terminal de usuario 1, una cámara web. Si el usuario no tiene una cámara web, se interrumpe la ejecución de la aplicación 30 y se elimina la aplicación de registro 31 del terminal de usuario 1 como si el usuario no estuviera autorizado a utilizar el servicio de verificación proporcionado por el tercero. Las aplicaciones adicionales (32, 33) no se descargan. En ese caso, la

sesión en línea con el servicio en línea 2 se ejecuta de manera convencional (es decir, sin verificación continua de la identidad del usuario).

Si el terminal de usuario 1 tiene una cámara web, cada vez que se inicia una sesión, se solicita preferiblemente al usuario que active la cámara web. Si el usuario se niega a activar la cámara web, se elimina la aplicación de registro 31 y se interrumpe la ejecución de la aplicación de control 30 (preferiblemente en la nube) como si el usuario no estuviera autorizado a utilizar el servicio de verificación proporcionado por el tercero. La sesión en línea con el servicio en línea 2 se ejecuta de manera convencional (es decir, sin verificación continua de la identidad del usuario).

Esta aplicación de registro 31 permite el acceso a la cámara web del terminal de usuario 1. Luego se ordena a la cámara tomar al menos una imagen (en teoría del usuario) y, una vez que el usuario acepta los términos y condiciones de uso, la al menos una imagen se envía junto con (asociada a) esos datos identificando inequívocamente al usuario tratando de establecer la sesión en el módulo de gestión 4 (flecha D1). Esos datos que identifican inequívocamente al usuario son preferentemente una ID de usuario. En una realización preferida, la cámara web toma y envía más de una imagen. De una manera más preferida, toma y envía tres imágenes. Como ya se explicó, los datos que identifican inequívocamente al usuario que está utilizando la sesión (preferentemente una ID de usuario) se proporcionan al terminal de usuario 1 (flecha A2) dentro de la orden para ejecutar la aplicación de control 30. De esta manera, la aplicación de control 30 conoce (a través del terminal de usuario 1) aquellos datos que identifican inequívocamente al usuario que está utilizando la sesión (preferentemente una ID de usuario). El terminal de usuario 1 los envía (flecha D1) al módulo de gestión 4 junto con la foto y los metadatos. Como ya se mencionó, estos datos (preferiblemente la ID de usuario) corresponden al usuario que ha iniciado sesión en el servicio en línea 2 con su identificador de usuario y contraseña. Esos datos son los datos del usuario que deben aparecer en las fotos (es decir, si no se produce ningún robo de identidad).

Una vez registrado, es decir, una vez que el tercero 20 tiene al menos una imagen (cara) del usuario del servicio web 2, el usuario puede cambiar sus fotos de registro siempre que lo desee, pero él/ella no está obligado/a a ello. Se recuerda que un usuario puede ser autorizado por el proveedor de servicios del servicio en línea 2 para usar el servicio de verificación facial proporcionado por el tercero 20, pero que aún no se ha registrado en ese servicio de verificación, porque aún no se ha conectado para el servicio de verificación primera vez al servicio en línea 2 ofrecido por el proveedor del servicio.

La al menos una imagen se almacena (flecha E3) en la base de datos 5 con sus metadatos asociados (datos que identifican inequívocamente al usuario (preferentemente una ID de usuario) y fecha/hora de captura). Posteriormente, el módulo de gestión 4 recoge la imagen(es) (flecha E4) y la/las transmite(n) (H1) a un módulo de entrenador facial 8. El módulo de entrenador facial 8 comprende un algoritmo automático de entrenamiento de reconocimiento facial, que está fuera del alcance de la presente invención. Crea un modelo biométrico de cada usuario registrado (en particular, de su cara) de las imágenes de registro. El módulo de entrenador facial 8 también es capaz de actualizar los modelos biométricos a partir de imágenes recibidas más recientemente de los usuarios. El módulo de entrenador facial 8 analiza las imágenes y crea un modelo biométrico del usuario a partir de la(s) imagen(es) registrada(s). Si el módulo de entrenador facial 8 detecta que en las fotografías tomadas en el proceso de registro (controlado por la aplicación 31) hay más de una cara, el registro no es válido y se ordena que la cámara web del terminal de usuario 1 tome nuevas fotos hasta que una foto permita el registro correcto (hasta que una foto comprenda una sola cara). El módulo de entrenador facial 8 envía (flecha H2) al módulo de gestión 4 el modelo biométrico creado, que luego se lleva (flecha E5) a la base de datos 5 y se almacena allí, finalizando el proceso de registro.

Una vez que se ha cumplido el proceso de registro, el módulo de aplicaciones 3 carga en el terminal de usuario 1 una aplicación interna 32 configurada para definir las preferencias de opciones de interacción entre la aplicación de toma de imágenes 33 y el terminal de usuario 1. Una vez que el usuario define sus opciones, se almacenan en la base de datos 5 a través del módulo de gestión 4 (flecha D2 desde el terminal de usuario 1 al módulo de gestión 4 y la flecha E14 desde el módulo de gestión 4 a la base de datos 5).

Finalmente, el módulo de aplicaciones 3 carga una aplicación interna 33 para tomar fotos durante todas las próximas sesiones. Esta aplicación 33 puede tomar fotos al azar o periódicamente. Además, puede informar al usuario que se va a tomar una foto o no. Por ejemplo, puede informar al usuario con una luz parpadeante o un sonido. Estos son parámetros definidos en las opciones entre la aplicación interna 32 y el terminal de usuario 1.

Caso 2: El usuario ya está registrado

Si el usuario ya está registrado, es decir, el proceso descrito en el caso 1 ya se ha producido una vez, la aplicación de control 30 da una orden de descargar (flecha B2) en el terminal de usuario 1 una aplicación 33 configurada para tomar fotos durante todas las próximas sesiones. En una realización preferida, esta aplicación 33 está configurada para tomar fotos aleatoriamente. Esta aplicación 33 se basa en la tecnología Flex de Adobe y es un desarrollo exclusivo de los inventores de la patente.

A continuación, si un usuario está autorizado por el proveedor de servicio para utilizar el servicio de verificación ofrecido por el tercero 20, la aplicación de registro 33 comprueba si el usuario tiene, en su terminal de usuario 1, una cámara web. Si el usuario no tiene una cámara web, la ejecución de la aplicación 30 se interrumpe y la aplicación 33 se elimina del terminal de usuario 1 como si el usuario no estuviera autorizado a utilizar el servicio de verificación proporcionado por el tercero. La aplicación adicional (32) no se descarga. En ese caso, la sesión en línea con el servicio en línea 2 se ejecuta de manera convencional (es decir, sin verificación continua de la identidad del usuario).

Si el terminal de usuario 1 tiene una cámara web, cada vez que se inicia una sesión, se solicita preferiblemente al usuario que active la cámara web. Si el usuario se niega a activar la cámara web, esta aplicación 33 se elimina y la ejecución de la aplicación de control 30 (preferiblemente en la nube) se interrumpe como si el usuario no estuviera autorizado a utilizar el servicio de verificación proporcionado por el tercero. La sesión en línea con el servicio en línea 2 se ejecuta de manera convencional (es decir, sin verificación continua de la identidad del usuario).

Esta aplicación 33 permite el acceso a la cámara web del terminal de usuario 1. Ya sea periódicamente o de vez en cuando (es decir, al azar alrededor de un tiempo medio) (esta segunda opción es la preferida), la aplicación 33 ordena a la cámara web tomar una foto (en teoría del usuario). La aplicación 33 envía luego la imagen junto con sus metadatos asociados (datos que identifican inequívocamente al usuario que está utilizando la sesión (preferentemente una ID de usuario) y la fecha/hora de captura) al módulo de gestión 4 (flecha D2). Como ya se explicó, los datos que identifican inequívocamente al usuario que está utilizando la sesión (preferiblemente una identificación de usuario) se proporciona (flecha A2) al terminal de usuario 1 dentro del orden para ejecutar la aplicación de control 30. De esta manera, la aplicación de control 30 conoce (a través del terminal de usuario 1) aquellos datos que identifican inequívocamente al usuario que está utilizando la sesión (preferentemente una ID de usuario). Estos datos (preferentemente una ID de usuario) corresponden al usuario que ha iniciado sesión en el servicio en línea 2 con su identificador de usuario y contraseña. Esos datos son los datos del usuario que deben aparecer en las fotos (es decir, si no se produce ningún robo de identidad). El terminal de usuario 1 los envía (flecha D2) al módulo de gestión 4 junto con la foto y los metadatos. Las imágenes que se envían al azar o periódicamente al módulo de gestión 4 se almacenan (flecha E6) en la base de datos 5 con los metadatos asociados (datos que identifican inequívocamente al usuario (preferentemente una ID de usuario) y fecha/hora de captura).

Posteriormente, el módulo de gestión 4 recoge la imagen almacenada (flecha E7) y la transmite (F1) a un módulo de reconocimiento facial automático 6. Este módulo 6 comprende un algoritmo convencional para el reconocimiento facial automático, que está fuera del alcance de la presente invención. La imagen y su modelo biométrico (que se extrae de la imagen en dicho módulo de reconocimiento 6) son analizados por el sistema de reconocimiento automático 6. Antes de comparar el modelo biométrico extraído con uno de referencia, el módulo de reconocimiento facial automático 6 detecta si la foto comprende al menos una cara o no y, si hay al menos una, cuántas de ellas hay. Una vez que se detectan una o más caras, procede a extraer las características faciales de cada cara para construir modelos biométricos correspondientes (construye un modelo para cada cara detectada en una imagen). El sistema de reconocimiento automático 6 recoge de la base de datos 5 un modelo biométrico de referencia de ese usuario. El modelo biométrico bajo análisis se compara así con el modelo biométrico de referencia que el sistema mantiene para ese usuario. El sistema de reconocimiento automático 7 entrega (flecha F2) un resultado del análisis (comparación de descriptores o parámetros faciales de la imagen con descriptores de referencia almacenados o modelo de parámetros del usuario, almacenados en la base de datos 5) hacia el módulo de gestión 4 que luego envía (flecha E8) el resultado a la base de datos 5 donde se almacena. El resultado es una variable cuyo valor proporciona toda la información necesaria para calificar el resultado. El módulo de gestión 4 ha establecido algunos rangos con posibles valores de esta variable. Según estos rangos, el módulo de gestión 4 sabe si ninguna persona aparece en una foto, si se detectó la persona adecuada, si se detectó una persona que no es la persona adecuada, si hay más de una persona en la foto, y así. En una realización particular, un usuario correctamente identificado da como resultado una variable con un entero positivo, en el que cuanto más cercano a 0 es el valor de la variable de resultado, más fiabilidad ofrece el sistema. En particular, el resultado se identifica como tener 100 % de precisión (garantía total de identificación correcta del usuario) o no tener una precisión del 100 % (incertidumbre en la identificación del usuario). Según el resultado entregado, el flujo de trabajo continúa de la siguiente manera:

a) Si el resultado entregado pertenece al grupo de precisión del 100 %, el resultado entregado se considera válido y el módulo de gestión 4 agrega al resultado una bandera que indica que no se necesita validación manual. El resultado se almacena en la base de datos 5 (flecha E9). Después de esto, el sistema pasa al estado de espera, esperando que se analice otra imagen.

b) Si el resultado entregado pertenece al grupo de resultados de incertidumbre, el módulo de gestión 4 agrega al resultado una bandera que indica que se necesita validación manual y la almacena (flecha E9) en la base de datos 5. Dos posibilidades surgen en este momento:

b1) Si la imagen es una imagen que requiere validación en tiempo real (que es algo que depende principalmente del tipo de servicio web 2 proporcionado por el proveedor del servicio), entonces el módulo de gestión 4 transmite (flecha G1) la imagen a un módulo de reconocimiento manual 7. Esto se explica en detalle más adelante.

b2) De lo contrario (si la imagen no requiere validación en tiempo real), el sistema pasa a estado en espera, a la espera de que otra imagen se analice.

Como se explica en relación con la variable que proporciona el resultado de la comparación facial, el sistema es capaz de determinar:

- Si la imagen es válida para el análisis (es decir, es capaz de excluir imágenes en negro)
- Si hay alguien frente a la webcam o no
- Si hay alguien, cuántas personas hay
- Si hay más de una persona, si una de ellas es la persona que debe estar frente a la pantalla
- Si solo hay una persona en la imagen, si esta persona es la persona que debería ser.

Esta determinación está fuera del alcance de la presente invención.

A continuación, se describe el caso en el que una imagen requiere validación manual en un módulo de reconocimiento manual 7. El módulo de reconocimiento manual 7 es una aplicación web para el reconocimiento facial manual que puede ser utilizado por el personal de un tercero. Por lo tanto, los miembros del personal pueden validar a los usuarios del servicio web y agrupar las imágenes. También verifica, a través del módulo de gestión 4, si el personal está autorizado para acceder a esta información.

El módulo de gestión 4 recoge (flecha E10) a partir de la base de datos 5 y envía (flecha G1) al módulo de reconocimiento manual 7 lo siguiente respecto de un usuario: imágenes pendientes de validación manual, las imágenes tomadas en el momento de registro de usuario y al menos una última imagen verificada. Además, puede enviar más de una imagen ya verificada.

El módulo de reconocimiento manual 7 tiene personal autorizado que necesita ser autorizado antes de comenzar a validar manualmente. Por ejemplo, están registrados con identificación y contraseña en la base de datos 5 y deben autenticarse en una aplicación de validación manual ubicada en el módulo de reconocimiento manual 7 y administrada por el módulo de gestión 4 que recopila datos de autenticación de la base de datos 5. Todas las imágenes servidas al personal están marcadas con técnicas de marca de agua. Esta marca se crea de acuerdo con el miembro del personal para identificar qué persona (miembro del personal) descarga qué imágenes de la base de datos 5. Por lo tanto, se evita el uso indebido de las imágenes.

La autenticación manual de imágenes se puede realizar en tiempo real o en tiempo no real (preferiblemente dentro de un período de tiempo limitado desde la captura de la imagen). En este último caso, las tareas se distribuyen según las premisas de un administrador de personal.

a) Si la verificación de la imagen debe realizarse en tiempo real: La imagen es analizada por el módulo de reconocimiento automático 6 y el módulo de gestión 4 (que es responsable de determinar si se necesita o no la verificación manual) almacena el resultado entregado en la base de datos 5. Después de esto, el módulo de gestión 4 envía la imagen (flecha G1) al módulo de reconocimiento manual 7. Este módulo 7 activa una alerta instantánea en un terminal de personal 9 (preferiblemente en un centro de llamadas para garantizar la respuesta en tiempo real). El terminal de personal 9 es un terminal utilizado por el personal para acceder a la aplicación web de validación manual 7 (módulo 7). El miembro del personal entrega un resultado de una validación visual de la imagen en tiempo real. El resultado de la verificación manual se almacena en la base de datos 5 por el módulo de gestión 4. En una realización preferida, más de un miembro del personal analiza la imagen para garantizar una identificación correcta del usuario.

b) Si no es necesario realizar una verificación de imagen en tiempo real: Las imágenes y los resultados del reconocimiento automático se almacenan en la base de datos 5. El personal responsable de verificar manualmente las imágenes puede hacerlo en cualquier momento. Cuando el personal accede (flecha I1) a través del terminal de personal 9 a una aplicación para el reconocimiento manual ubicado en el módulo de reconocimiento manual 7, este módulo 7 solicita (flecha G3) al módulo de gestión 4 un conjunto de imágenes pendientes de validación manual. El módulo de gestión 4 recoge (flecha E10) las imágenes de la base de datos 5 e inserta las correspondientes marcas de agua en ellas. El módulo de gestión 4 sirve (flecha G4) esta información al terminal de personal 9 (flecha I2) utilizando la aplicación para el reconocimiento manual.
Usando la aplicación de reconocimiento manual 7, el personal entrega los resultados de verificación manual (flechas I3 G5) al módulo de gestión 4 que se almacenan (flecha E11) en la base de datos 5. Para asegurar que todos los miembros del personal estén haciendo su trabajo adecuadamente, el módulo de gestión 4 sirve cada imagen a diferentes miembros del personal. De esta forma, compara los resultados entregados, que deben ser los mismos. Si los resultados son diferentes, el módulo de gestión 4, responsable de esta comprobación, continúa sirviendo imágenes hasta que se validan correctamente. Registra además en la base de datos 5 contadores que cuentan la cantidad de veces que una imagen ha sido evaluada y por quién. Para cada miembro del personal y cada proceso de validación, el módulo de gestión 4 actualiza en la base de datos 5 un contador correspondiente de imágenes servidas e imágenes validadas manualmente.

Una vez que una imagen ha sido (preferiblemente de forma manual, pero alternativamente solo automáticamente) verificada como correcta (es decir, se ha verificado que una imagen corresponde al usuario que se registró originalmente en el servicio web 2), la gestión el módulo 4 toma (flecha E12) la imagen verificada de la base de datos 5 al módulo de entrenador facial 8 (flecha H3). En este módulo de entrenador facial 8 se crea un nuevo modelo biométrico del usuario registrado, basado en las imágenes de usuario verificadas recientes, actualizando así el modelo biométrico creado cuando el usuario se registró por primera vez. Posteriormente, el modelo biométrico resultante se almacena (flecha H4, E13) en la base de datos 5 (a través del módulo de gestión 4).

El tercero 20 presenta los resultados de verificación según lo requiere el proveedor de servicios 2. Los resultados están organizados por un módulo de presentación de resultados 10 propiedad de un tercero 20. El módulo 10 transforma los valores numéricos almacenados en la base de datos 5 en representaciones gráficas y tablas. El módulo de presentación de resultados 10 del tercero 20 envía los resultados del módulo de gestión 4 a un terminal 11 del proveedor de servicios. El proveedor de servicios utiliza este terminal 11 para acceder a la aplicación web de presentación de resultados. Esto se hace a pedido de forma periódica. En una realización preferida, el tercero 20 genera automáticamente informes periódicos. Estos informes son generados en particular por el módulo 10, que toma la información requerida de la base de datos 5 a través del módulo de gestión 4. El módulo 10, de manera periódica o en respuesta a una alarma que se activa cuando un determinado comportamiento definido por el proveedor de servicios en línea falla envía periódicamente los informes al proveedor de servicios en línea. En una realización particular, se envían por correo electrónico. El acceso a los resultados está restringido a los proveedores autorizados. Por esta razón, el proveedor de servicios 2 debe identificarse, por ejemplo, mediante una ID y una contraseña, que se verifican en la base de datos 5 de manera similar a los miembros del personal en la etapa de verificación manual. Una vez autorizado a través del módulo de presentación de resultados 10, el proveedor de servicios en el terminal 11 solicita (flecha K1) los resultados al módulo de presentación 10 que a su vez los recoge (flecha J1) del módulo de gestión 4. Esto los recoge de la base de datos 5 y los envía al módulo de presentación 10, que entrega los resultados al terminal 11 (flecha J2, K2). Preferiblemente crea gráficos, cuadros y tablas que se sirven para su visualización en el terminal 11 como una página web dinámica.

En una realización preferida, todos los servidores y bases de datos del tercero 20 están en la nube. Alternativamente, los servidores y las bases de datos son servidores locales y bases de datos.

Todas las comunicaciones entre el usuario final (en el terminal de usuario 1) y el tercero (flechas B y D), entre el personal y el tercero (flechas I), entre el proveedor de servicios y el tercero (flechas K) y entre el usuario final (en el terminal de usuario 1) y el proveedor de servicios (flechas A) son preferiblemente protocolos TCP/IP, http y POST.

La transmisión de información en estos canales de comunicaciones está codificada. Todas las comunicaciones de resto son intra servidor, cable físico. Todas las peticiones de acceso desde diferentes terminales deben ir acompañadas de la ID correspondiente (usuario, personal o proveedor) para la autorización. Todas las imágenes, tanto en comunicaciones internas como externas, siempre van acompañadas de una identificación del usuario que debe aparecer en la imagen.

El sistema asegura así resultados válidos con un 100 % de precisión, gracias a la combinación de módulos de verificación automática y manual.

Además, el sistema funciona las 24 horas del día, los 365 días del año. Además, es un sistema multilingüe y accesible desde cualquier parte del mundo, siempre que se disponga de acceso a Internet.

En este texto, el término "comprende" y sus derivaciones (tales como "que comprende", etc.) no deben entenderse en un sentido excluyente, es decir, estos términos no deben interpretarse como excluyentes de la posibilidad de que lo que descrito y definido puede incluir otros elementos, etapas, etc.

Por otro lado, la invención no está obviamente limitada a la(s) realización(es) específica(s) descrita(s) en este documento, sino que también abarca cualquier variación que pueda ser considerada por cualquier persona experta en la técnica (por ejemplo, en lo que respecta a la elección de materiales, dimensiones, componentes, configuración, etc.), dentro del alcance general de la invención como se define en las reivindicaciones.

REIVINDICACIONES

1. Un método para verificar la identidad de un usuario de un servicio en línea, **caracterizado por** las etapas de:

- cuando un terminal de usuario (1) está conectado (A1) a un servicio en línea (2) por medio de una comunicación a través de un protocolo de Internet, enviar (A2) desde un servidor de dicho servicio en línea (2) a dicho terminal de usuario (1) una dirección IP de un servidor de autenticación (3);
- conectar (B1) dicho terminal de usuario (1) a dicha dirección IP y descargar (B2) de dicho servidor de autenticación (3) al menos una aplicación (33), siendo dicha al menos una aplicación (33) para tomar fotos con la cámara web del terminal de usuario (1);
- tomar una foto con la cámara web del terminal de usuario (1), siendo dicha toma de la foto controlada por dicha aplicación (33);
- enviar (D2) dicha foto y metadatos asociados a una unidad de gestión (4), comprendiendo dichos metadatos al menos una ID de usuario del usuario que usa dicho terminal de usuario (1) y la hora de captura de dicha foto;
- almacenar (E6) dicha foto y metadatos asociados en una base de datos (5);
- en un módulo de reconocimiento facial automático (6), extraer automáticamente un conjunto de parámetros biométricos por cada cara que aparece en dicha foto;
- en dicho módulo de reconocimiento facial automático (6), comparar dicho conjunto o conjuntos de parámetros biométricos extraídos de dicha fotografía con un modelo biométrico de referencia del usuario al que pertenece dicha ID de usuario, almacenándose dicho modelo de referencia biométrico en dicha base de datos (5);
- si en el resultado de dicha comparación la persona en la foto coincide inequívocamente con el usuario al que pertenece dicha ID de usuario, dicha unidad de gestión (4) agrega al resultado una bandera que indica que no se necesita ninguna validación manual;
- de lo contrario, si en el resultado de dicha comparación la persona de la foto no coincide inequívocamente con el usuario al que pertenece dicha ID de usuario, la unidad de gestión (4) agrega al resultado una bandera que indica que se necesita validación manual; después: informando de esto al proveedor de servicios en línea (2) o enviando (G1) dicha foto a una unidad de reconocimiento manual (7) para la validación manual de la foto;
- repetir la etapa de tomar una foto con la cámara web del terminal de usuario (1) y las etapas subsiguientes, verificando continuamente la identidad del usuario conectado al servicio en línea (2) a través de dicho terminal de usuario (1).

2. El método de la reivindicación 1, en el que dicha etapa de repetir la toma de una fotografía con la cámara web del terminal de usuario (1) se realiza aleatoriamente.

3. El método de la reivindicación 1, en el que dicha etapa de repetir la toma de una foto con la cámara web del terminal de usuario (1) se realiza periódicamente.

4. El método de cualquier reivindicación anterior, en el que el terminal de usuario (1) proporciona la ID de usuario del usuario que usa dicho terminal de usuario (1) que se envía (D2) a una unidad de gestión (4) junto con dicha fotografía que a su vez se ha obtenido (A2) de dicho proveedor de servicios en línea.

5. El método de cualquier reivindicación anterior, en el que si el usuario todavía no ha sido registrado como usuario de dicho servicio en línea (2), antes de descargar desde dicho servidor de autenticación (3) una aplicación (33) para tomar fotos con la cámara web del terminal de usuario (1):

- se descarga una aplicación (31) para el registro en una sesión controlada de reconocimiento facial desde dicho servidor de autenticación (3) a dicho terminal de usuario (1), estando dicha aplicación de registro (31) configurada para tomar al menos una primera fotografía con la cámara web del terminal de usuario (1);
- se toma al menos una primera fotografía con la cámara web del terminal de usuario (1), estando dicha toma controlada por dicha aplicación de registro (31);
- dicha al menos una primera foto y metadatos asociados se envían (D1) a la unidad de gestión (4), siendo dichos metadatos al menos una ID de usuario del usuario que usa dicho terminal de usuario (1) y la hora de captura de dicha al menos una primera foto;
- almacenar (E3) dicha al menos una primera fotografía y metadatos asociados en dicha base de datos (5);
- para dicha al menos una primera fotografía, crear (8) mediante un algoritmo de entrenamiento automático de reconocimiento facial un modelo biométrico de la cara comprendida en dicha foto;
- almacenar (E5) el modelo biométrico creado en dicha base de datos (5), finalizando el proceso de registro.

6. El método de la reivindicación 5, que comprende además la etapa de, una vez que se ha verificado que una foto pertenece al usuario que se registró originalmente en el servicio en línea (2), crear un modelo biométrico actualizado del usuario registrado de dicha foto verificada y almacenar (H4, E13) dicho modelo biométrico actualizado en dicha base de datos (5).

7. El método de cualquiera de las reivindicaciones 5 o 6, en el que, en dicha etapa de crear (8) mediante un algoritmo automático de entrenamiento de reconocimiento facial, un modelo biométrico de la cara comprendida en dicha foto, si se detecta que hay más de una cara en la foto, el registro no es válido y se ordena que la cámara web

del terminal de usuario (1) tome nuevas fotos hasta que una fotografía comprenda una sola cara.

8. El método de cualquier reivindicación anterior, que comprende además la etapa de descargar (B2) desde dicho servidor de autenticación (3) una aplicación (32) para definir algunas preferencias en la interacción entre la aplicación para tomar fotos (33) y el terminal de usuario (1)).

9. El método de cualquier reivindicación anterior, en el que dicha aplicación (31, 32, 33) descargada en dicho terminal de usuario (1) desde dicho servidor de autenticación (3) es una aplicación portátil ejecutada en dicho terminal de usuario (1) sin estar instalada en el mismo.

10. El método de cualquier reivindicación anterior, en el que, si dicha fotografía se toma (G1) en una unidad de reconocimiento manual (7) para la validación manual de la foto, a dicha unidad de reconocimiento manual (7) se accede mediante un validador humano desde un terminal remoto (9).

11. Un sistema para verificar la identidad de un usuario de un servicio en línea, **caracterizado por que** comprende:

- un servidor de autenticación (3) configurado para proporcionar a un terminal de usuario (1), a través del cual un usuario puede conectarse a un servicio en línea (2), al menos una aplicación (33), siendo dicha al menos una aplicación (33) una aplicación para tomar fotos con una cámara web del terminal de usuario (1);
- una unidad de gestión (4) configurada para recibir una fotografía tomada por dicha cámara web a petición de dicha aplicación (33) y metadatos asociados, comprendiendo dichos metadatos al menos un ID de usuario del usuario que usa dicho terminal de usuario (1) y la hora de captura de dicha foto;
- una base de datos (5) para almacenar dicha foto y dichos metadatos asociados y una colección de fotos y modelos biométricos correspondientes de usuarios registrados de dicho servicio en línea (2);
- una unidad de reconocimiento automático (6) configurada para extraer un conjunto de parámetros biométricos por cada cara que aparece en dicha foto y para comparar dicho conjunto o conjuntos de parámetros biométricos extraídos de dicha foto con un modelo biométrico de referencia del usuario al cual pertenece dicha ID de usuario, siendo dicho modelo biométrico de referencia almacenado en dicha base de datos (5);

en donde dicha unidad de gestión (4) también está configurada, si en el resultado de dicha comparación la persona en la foto coincide inequívocamente con el usuario al que pertenece dicha ID de usuario, para agregar al resultado una bandera que indica que no se necesita validación manual, y, si en el resultado de dicha comparación la persona en la foto no coincide inequívocamente con el usuario al que pertenece dicha ID de usuario, para agregar al resultado una bandera que indica que se necesita validación manual;

- una unidad de validación manual (7) para validar la foto en caso de que la comparación automática no sea capaz de coincidir inequívocamente la persona de la foto con una persona autorizada.

12. El sistema de la reivindicación 11, en el que dicho servidor de autenticación (3), dicha unidad de gestión (4), dicha base de datos (5), dicha unidad de reconocimiento automático (6) y dicha unidad de reconocimiento manual (7) están en la nube.

13. El sistema de cualquiera de las reivindicaciones 11 o 12, que comprende además un módulo de entrenador facial (8) que comprende un algoritmo de entrenamiento automático de reconocimiento facial y configurado para crear un modelo biométrico de cada usuario registrado de al menos una fotografía.

14. El sistema de la reivindicación 13, en el que dicho módulo de entrenador facial (8) está configurado para actualizar los modelos biométricos a partir de las fotos recibidas más recientemente de los usuarios.

15. Producto de programa informático que comprende instrucciones/código de programa informático para realizar el método de acuerdo con cualquiera de las reivindicaciones 1 a 10.

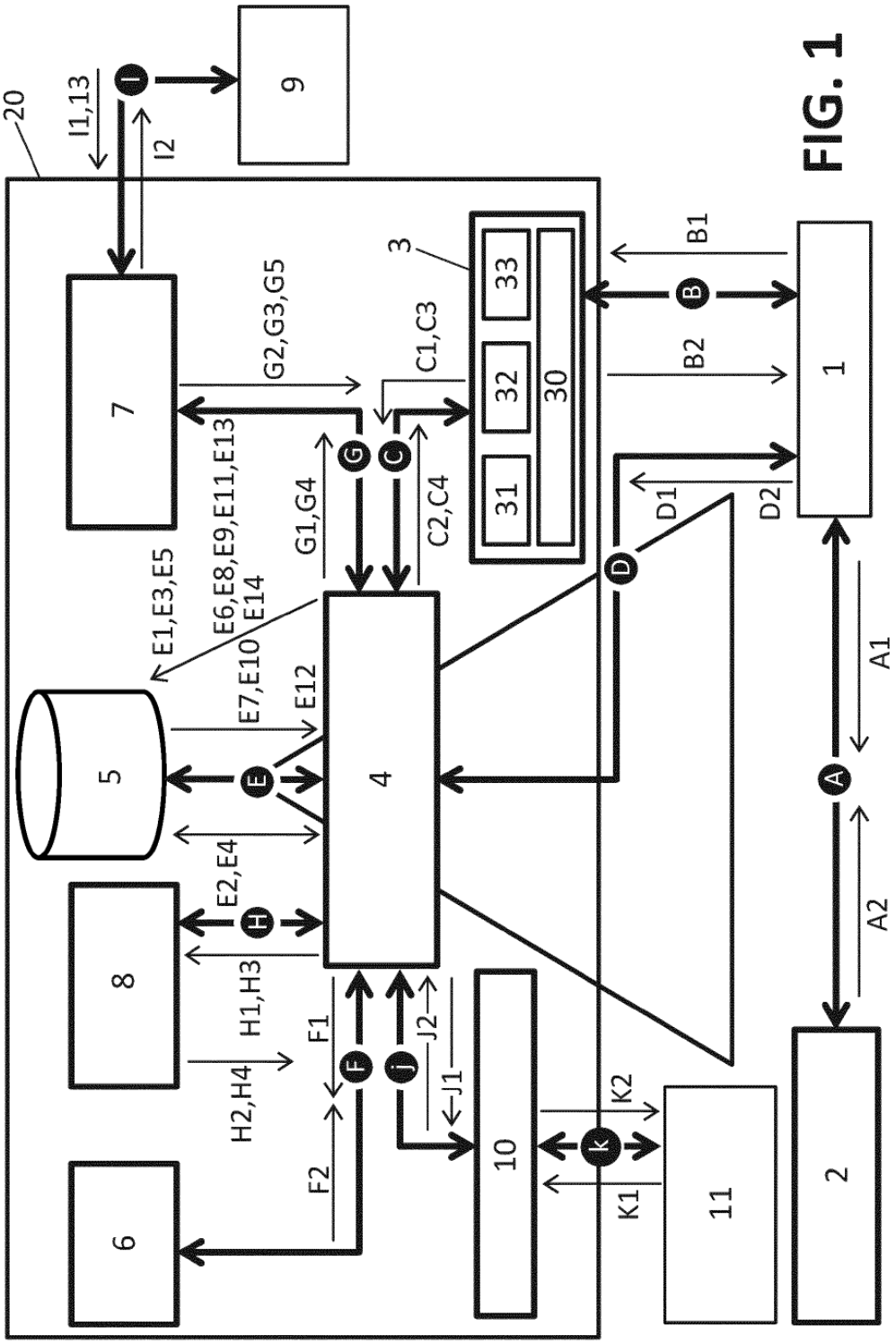
20
I1,13
I2
I
9
7
G2,G3,G5
C1,C3
3
33
32
30
31
B1
B
B2
1
G
C
G1,G4
C2,C4
D1
D2
D
E1,E3,E5
E6,E8,E9,E11,E13
E14
E7,E10
E12
5
E
4
A1
A
A2
E2,E4
H
8
H1,H3
F1
F
J2
J
J1
H2,H4
F2
10
K2
K
K1
11
2
6

FIG. 1