(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 791 776**

(51) Int. CI.:

G06K 9/46 (2006.01)
G06K 9/62 (2006.01)
H04L 29/06 (2006.01)
G06F 21/32 (2013.01)
G06K 9/00 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.09.2013 PCT/US2013/058343**

(87) Fecha y número de publicación internacional: **13.03.2014 WO14039732**

(96) Fecha de presentación y número de la solicitud europea: **05.09.2013 E 13834699 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.02.2020 EP 2893489**

(54) Título: **Sistema y método para la autenticación biométrica en conexión con dispositivos equipados con cámara**

(30) Prioridad:

05.09.2012 US 201261696820 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.11.2020

(73) Titular/es:

ELEMENT, INC. (100.0%)
72 Greene Street Fl. 4
New York NY 10012, US

(72) Inventor/es:

LECUN, YANN;
PEROLD, ADAM;
WANG, YANG y
WAGHMARE, SAGAR

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Sistema y método para la autenticación biométrica en conexión con dispositivos equipados con cámara

Referencia cruzada a aplicaciones relacionadas

Esta solicitud se basa en, y reivindica el beneficio de la fecha de presentación de la solicitud de patente provisional U.S. número 61/696,.820, presentada el 5 de septiembre de 2012.

Antecedentes de la invención

Campo de la invención

La presente invención se refiere en general al uso de tecnología biométrica para autenticación e identificación, y más particularmente a soluciones sin contacto para autenticar e identificar usuarios, a través de ordenadores, tales como dispositivos móviles, para permitir o denegar selectivamente el acceso a diversos recursos. En la presente invención, la autenticación y/o identificación se realiza usando una imagen o un conjunto de imágenes de la palma de un individuo a través de un proceso que involucra las siguientes etapas clave: (1) detectar el área de la palma usando clasificadores locales; (2) extraer características de las regiones de interés; y (3) calcular el puntaje de comparación contra los modelos de usuario almacenados en una base de datos, que pueden aumentarse dinámicamente a través de un proceso de aprendizaje.

Discusión de la técnica relacionada

Los dispositivos móviles, tales como teléfonos inteligentes, tabletas y ordenadores portátiles, han sido ampliamente adoptados y utilizados por muchas personas a diario. Estos dispositivos se han vuelto cada vez más potentes y, a medida que los desarrolladores crean más y más aplicaciones y servicios que se ejecutan en ellos, se vuelven aún más arraigados en nuestra vida cotidiana. Estos dispositivos móviles no solo proporcionan una poderosa plataforma informática por derecho propio, sino que también brindan conectividad a un conjunto prácticamente ilimitado de servicios, aplicaciones y datos disponibles en plataformas remotas a las que típicamente se accede a través de un enlace inalámbrico a un sitio celular y luego se devuelven a la columna vertebral de internet. Además de acceder a estas plataformas remotas, los dispositivos móviles también tienen la capacidad de conectarse a otros dispositivos móviles a través de conexiones inalámbricas de corto y largo alcance.

Quizás lo más importante es que la penetración cada vez mayor de estos dispositivos, combinada con la reducción continua de los costes asociados con las partes componentes de estos dispositivos, ha dado como resultado que los dispositivos estén disponibles con mayores capacidades sin dejar de ser asequibles para muchos usuarios. Por ejemplo, como resultado de la reducción en los costes de las partes componentes y el desarrollo de un software más potente, un número sustancial de teléfonos inteligentes ahora incluye cámaras potentes, que pueden tomar fotos extraordinariamente detalladas del orden de ocho megapíxeles o más.

Una cuestión importante que surge en el contexto de los dispositivos móviles y su uso generalizado en relación con tanta funcionalidad y su necesidad de interactuar con tantos recursos diferentes es la necesidad de controlar el acceso a cada uno de estos recursos para que solamente aquellos individuos o dispositivos que deben estar autorizados para acceder a los recursos aplicables, realmente puedan hacerlo. En el caso típico, el acceso a los recursos se controla mediante la entrada de cadenas de texto/numéricas, tales como ID de usuario y contraseñas. Por ejemplo, se le puede solicitar al usuario de un teléfono inteligente que ingrese un código de cuatro dígitos antes de que se le permita acceder a cualquier funcionalidad en el dispositivo. Además, cada aplicación local u otro recurso en el dispositivo puede requerir que el usuario ingrese una o más cadenas de texto/numéricas antes de obtener acceso al recurso. En este caso, los datos correctos (ID de usuario, contraseña, etc.) pueden almacenarse en la memoria del dispositivo. Alternativamente, para el acceso a los recursos (aplicaciones, datos, capacidades de comunicación, etc.) que se encuentran remotamente desde el dispositivo, el usuario y/o el dispositivo podrían tener que transmitir un conjunto correcto de cadenas de texto/numéricas al recurso remoto que, a su vez, verifica que los datos transmitidos coincidan con los datos correctos antes de permitir el acceso al recurso.

Como se podría imaginar, para un usuario típico de un teléfono inteligente, por ejemplo, hay un número de inconvenientes con las técnicas anteriores para la autenticación e identificación. Por un lado, la necesidad de recordar identificaciones de usuario y contraseñas para tantas aplicaciones, servicios y otros recursos diferentes, teniendo cada uno sus propios requisitos sobre cómo deben construirse esas identificaciones y contraseñas, puede ser bastante desalentador y los usuarios a menudo olvidan sus identificaciones y contraseñas para recursos a los que no acceden con frecuencia. Otra desventaja es que existen problemas de seguridad con el uso de cadenas de texto/numéricas para controlar el acceso a los recursos. Hay, por ejemplo, potentes programas de software que pueden usarse para provocar intrusión en estas cadenas para obtener acceso no autorizado a los recursos.

Además, el método típico con base en contacto de un usuario que usa sus dedos para ingresar contraseñas e ID de usuario en la pantalla del teléfono inteligente se presta a riesgos de seguridad. Los intrusos informáticos experimentados a menudo pueden "levantar" el patrón de huellas digitales de la pantalla con base en el residuo de aceite que deja el dedo para obtener acceso no autorizado. Esto es particularmente cierto en el contexto de ingresar

una cadena numérica corta tal como un número de cuatro dígitos para desbloquear el dispositivo. Una vez que se desbloquea el dispositivo, es posible que muchos de los recursos del dispositivo ni siquiera estén asegurados, lo que conlleva graves riesgos de seguridad.

Una solución que se ha dirigido para eliminar o reducir los inconvenientes discutidos anteriormente implica el uso de tecnología biométrica para controlar el acceso a los recursos disponibles a través de dispositivos móviles. Si bien estas soluciones, en algunos casos, han eliminado algunos de los inconvenientes discutidos anteriormente, todavía sufren un número de desventajas. Por ejemplo, algunas soluciones con base en contactos requieren que un usuario coloque su dedo en el sensor del dispositivo, el cual tiene la capacidad de capturar la huella digital del usuario, la cual es luego comparada contra los datos de huellas digitales locales o ubicadas remotamente para determinar si hay una coincidencia suficiente para permitir que el usuario o el dispositivo accedan a uno o más recursos. En este caso, como se mencionó anteriormente, un intruso informático puede levantar una huella digital del sensor del dispositivo y utilizarla para obtener acceso no autorizado a uno o más recursos en un momento más adelante utilizando esa huella digital apropiada. Estas soluciones típicamente también sufren del inconveniente de que el tiempo para realizar el procesamiento necesario para determinar si la huella digital es una coincidencia puede ser inaceptable en el contexto de un usuario ocupado que intenta obtener acceso a muchos recursos diferentes en el dispositivo durante el transcurso de un día típico.

Existen problemas de salud adicionales asociados con los métodos con base en contacto que implican la transmisión de gérmenes, virus u otros peligros biológicos, particularmente en el caso de dispositivos compartidos entre usuarios. Como se sabe en la técnica, las yemas de los dedos de un individuo, y las manos de un individuo más en general, son a menudo uno de los medios principales para transferir gérmenes, virus u otros peligros biológicos entre las personas. En el caso de dispositivos individuales que se comparten entre múltiples personas, métodos de autenticación e identificación con base en contacto en los que un usuario escribe una cadena de identificación con la punta de sus dedos, o se autentica o se identifica a sí mismo a través de métodos biométricos con base en contacto, tal como el reconocimiento de huellas digitales o huellas de la palma, entre otros, crea el riesgo de transferir dichos riesgos biológicos a través del medio de contacto compartido.

El documento EP2192526 A2 divulga un dispositivo y método de autenticación biométrica que incluye extraer información de movimiento que representa la flexión y el estiramiento de un objeto de imagen a partir de una pluralidad de imágenes obtenidas, y determinar si el objeto de imagen es o no un objeto biológico, con base en la información de movimiento.

Resumen de la invención

Es por lo tanto, un objeto de la invención proporcionar un sistema biométrico y metodología sin contacto que admita la autenticación e identificación precisa, segura y rápida de usuarios y dispositivos para proporcionar acceso selectivo a recursos accesibles a través de dispositivos equipados con cámara.

En una realización de la presente invención, los usuarios de tales dispositivos equipados con cámara (en lo sucesivo denominados en ocasiones "teléfonos inteligentes" por conveniencia, aunque debe entenderse que los dispositivos incluyen todos los dispositivos con capacidad de cámara, incluidos tanto dispositivos móviles como dispositivos estacionarios, tales como ordenadores de escritorio) que deben identificarse o autenticarse a sí mismos como condición para obtener acceso a uno o más recursos, tomar una o una serie de fotos de su palma o ambas palmas usando la cámara del teléfono inteligente. El sistema de la presente invención emplea entonces tecnología de visión por ordenador para analizar la imagen de la huella de la palma de la mano y verificar bien sea que la firma de la huella de la palma coincida con el modelo del usuario en una base de datos (autenticación del usuario) o encontrar el modelo de usuario que coincida entre muchos modelos en una base de datos (identificación de usuario).

Características y aspectos adicionales de la presente invención se harán evidentes a partir de la siguiente descripción detallada de realizaciones de ejemplo en relación con la referencia a las figuras adjuntas.

Breve descripción de los dibujos

La figura 1 es un diagrama que representa los componentes principales del sistema de la presente invención en una realización preferida de la misma;

La figura 2 es un diagrama de bloques, que es útil para ilustrar la metodología de la presente invención en una realización preferida de la misma;

La Figura 3 es un diagrama que ilustra la conectividad segura entre un dispositivo móvil y uno o más servidores remotos de acuerdo con una realización preferida de la presente invención;

La Figura 4 es un diagrama de flujo que ilustra las etapas clave en la autenticación de un usuario o dispositivo de acuerdo con la presente invención en una realización preferida de la misma; y

La figura 5 es un diagrama de flujo que ilustra las etapas clave en la autenticación de un usuario o dispositivo de acuerdo con la presente invención en una realización preferida de la misma.

Descripción detallada de realizaciones de ejemplo

Ahora se hará referencia en detalle a diversas realizaciones de ejemplo de la invención. Debe entenderse que la siguiente discusión de realizaciones de ejemplo no pretende ser una limitación de la invención, como se divulga ampliamente aquí. Más bien, la siguiente discusión se proporciona para proporcionar al lector una comprensión más detallada de ciertos aspectos y características de la invención.

Antes de que las realizaciones de la presente invención se describan en detalle, debe entenderse que la terminología utilizada en este documento tiene el propósito de describir solamente realizaciones particulares, y no pretende ser limitante. A menos que se defina otra cosa, todos los términos técnicos utilizados en este documento tienen el mismo significado que comúnmente entiende un experto en la técnica a la que pertenece el término. Aunque cualquier método y material similar o equivalente a los descritos en este documento se puede usar en la práctica de la presente invención, ahora se describen los métodos y materiales preferidos. Todas las publicaciones mencionadas aquí se incorporan aquí como referencia para divulgar y describir los métodos y/o materiales en relación con los cuales se citan las publicaciones. La presente divulgación controla en la medida en que entre en conflicto con cualquier publicación incorporada.

Como se usa en este documento y en las reivindicaciones adjuntas, las formas singulares "un", "uno, una" y "el, la" incluyen referentes plurales a menos que el contexto indique claramente otra cosa. Así, por ejemplo, la referencia a "una palma" incluye una sola palma o ambas palmas de un individuo y la referencia a "una imagen" incluye referencia a una o más imágenes. Adicionalmente, el uso de términos que pueden describirse usando términos equivalentes incluye el uso de esos términos equivalentes. Así, por ejemplo, debe entenderse que el uso del término "cámara" incluye cualquier dispositivo capaz de obtener una imagen de un objeto. Como otro ejemplo, y como se mencionó anteriormente, el término "teléfono inteligente" incluye todos los dispositivos con una capacidad de cámara.

A continuación se presenta una descripción de la presente invención en realizaciones preferidas de la misma. Con referencia a la Figura 1, ahora sigue una discusión de los componentes clave del sistema de la presente invención, así como el contexto en el que cada uno de estos componentes interactúa entre sí para obtener las ventajas de la presente invención. El Dispositivo 100 puede ser cualquier dispositivo que contenga una cámara capaz de tomar fotografías de alta calidad. Preferiblemente, la cámara del Dispositivo 100 también contiene un elemento de *flash* capaz de activarse y desactivarse selectiva y rápidamente para iluminar el área que se va a fotografiar. Ejemplos de tales Dispositivos 100 incluyen teléfonos inteligentes, tabletas, ordenadores portátiles y cualquier otro dispositivo que pueda llevar un usuario y que proporcione una plataforma informática que permita que la funcionalidad de la presente invención sea operativa, así como ordenadores de escritorio o un variedad de dispositivos estacionarios integrados. Ejemplos de tales dispositivos integrados estacionarios incluyen equipos de cámara fijos a las entradas de las instalaciones u otras ubicaciones estratégicas que proporcionan acceso seguro a espacios físicos u otros recursos, o equipos de cámara fijos a ubicaciones estratégicas para fines tales como protocolos de tiempo y asistencia, así como otras aplicaciones. Aunque no es obligatorio, el Dispositivo 100 también puede contener otras diversas características, tales como una pantalla de visualización (que también puede ser una pantalla táctil), un teclado, un acelerómetro, capacidades de GPS, capacidad de almacenamiento y una unidad central de procesamiento (CPU).

El Dispositivo 100 incluye al menos una Cámara 105, que es preferiblemente capaz de producir fotografías de alta calidad de, por ejemplo, dos megapíxeles o más, tal como cuatro megapíxeles, seis megapíxeles u ocho megapíxeles. El Procesador de Datos de Cámara 110 recibe los datos de imagen de la Cámara 105 y los procesa como se conoce en la técnica para crear datos de píxeles representativos de la fotografía, que pueden usarse de diversas maneras, incluso para los fines descritos en relación con la presente invención como se describe ahora. Los datos del Procesador de Datos de Cámara 110 alimentan al Detector de Región de Interés 115, que sirve para ubicar el área de la palma dentro de la imagen más amplia y delinear el área con un alto nivel de precisión y consistencia, tal como para proporcionar máscaras de área de la palma de sustancialmente la misma forma y posición en la palma a través de una variedad de imágenes independientes con diferentes condiciones de iluminación y orientaciones de la palma hacia la cámara.

En una realización de Detector de Región de Interés 115, la región de interés se detecta usando clasificadores locales con base en ventanas deslizantes para etiquetar los píxeles de la palma y los que no son de la palma por los puntajes de clasificación, seguido de una etapa de segmentación para agrupar los píxeles de la palma vecinos en componentes conectados en la imagen de entrada. Se puede lograr un alto nivel de precisión y robustez con respecto al ruido de la imagen porque se aprende un número significativo de características locales discriminatorias a partir de una gran colección de imágenes de ejemplo para capturar las características estables de la apariencia de la palma para formar clasificadores fuertes. Como resultado, el detector entrenado puede localizar y delinear con precisión las regiones de interés en las imágenes de entrada tomadas de forma libre con diversas orientaciones manuales y condiciones de iluminación.

En una realización del Detector de Región de Interés 115, se usan clasificadores locales basados en Haar Wavelets y AdaBoost (referencia 1) para detectar la región de interés en el área de la palma de la mano de un usuario. En otra realización del Detector de Región de Interés 115, se usan clasificadores locales basados en máquinas de vectores de soporte (referencia 2) para detectar la región de interés en el área de la palma de la mano de un usuario. En otra realización del Detector de Región de Interés 115, se usa una red neuronal convolucional para detectar la región de

interés en el área de la palma de la mano de un usuario, tal como las descritas en las Patentes U.S. Nos. 5,067,164 y 5,058,179, y en (referencias 3 y 4).

El Detector de Región de Interés 115 alimenta entonces los datos de la imagen, incluida la máscara del área de la palma, al Procesador de Conversión 120, que sirve para extraer una Firma 125 de los parches de imagen que representan los rasgos característicos del área de la palma del individuo que puede usarse para distinguir al individuo del otro usuario, en el que dichos parches son pequeñas ventanas de muestreo dentro de la máscara del área de la palma.

En una realización, la Firma 125 es un vector calculado de la siguiente manera. Primero, se calcula un histograma de orientaciones de bordes en un número de regiones bien elegidas de la imagen. Esto se puede realizar utilizando uno de los métodos bien conocidos de visión por ordenador para extraer descriptores de imágenes locales, tales como la Transformación de Características Invariables de Escala (SIFT) (véase, por ejemplo, referencia 5), Histograma de Gradientes Orientados (HOG) (véase, por ejemplo, referencia 6), y otras referencias conocidas en la técnica. En segundo lugar, cada histograma de orientación se compara con un número de prototipos que se han calculado a partir de datos de entrenamiento, por ejemplo, utilizando el bien conocido algoritmo de agrupamiento de K-medias. Finalmente, el vector de firma se forma de tal manera que el componente k del vector corresponde al prototipo k-ésimo mencionado anteriormente. El componente k contiene el número de regiones para las cuales el histograma estaba más cerca del prototipo k que de todos los demás prototipos. Esta secuencia de operaciones se conoce en la literatura como una representación de "Bolsa de características" (véase la referencia 7, por ejemplo). Debería ser evidente a partir de las enseñanzas actuales que en otra realización de la presente invención, se pueden usar múltiples Bolsas de Características para preservar la relación geométrica entre regiones locales.

La Firma 125 es entonces alimentada al Motor de Autenticación e Identificación (Motor AID) 130, el cual sirve para implementar muchos de los procesos clave de la presente invención como se describe aquí más adelante. El Motor AID 130 se comunica con la Base de datos de los Modelos de Usuario 135, si está presente, para almacenar una copia local de un modelo de usuario. Por lo tanto, en el caso de aplicaciones o servicios que residen localmente en el Dispositivo 100 y no requieren comunicación externa con, por ejemplo, servidores remotos o dispositivos remotos, una firma del usuario resultante de las imágenes de huella de la palma tomadas por la Cámara 105 se puede comparar con los modelos de usuario conocidos, almacenados en la Base de Datos de Modelos de Usuario 135 para autenticación o identificación. Los modelos de usuario son modelos estadísticos calculados a partir de una colección de imágenes de la palma de un individuo, con las firmas derivadas de esas imágenes que definen el modelo. En una realización, el modelo de usuario consiste en un denominado modelo de densidad Gaussiana de las firmas calculadas a partir de las imágenes de referencia del usuario. Dada la firma de la imagen de consulta S, el modelo de usuario se utiliza para calcular una puntuación coincidente. Se considera que la firma coincide con el modelo de usuario si la puntuación coincidente

$$R = \sum_i \frac{(Si - Mi)^2}{Vi+u}$$

donde Mi y Vi son la media y la varianza del componente i-ésimo de los vectores de firma de todas las imágenes de referencia del usuario dado, y u es una pequeña constante. Se considera que la firma es coincidente con el modelo de usuario si la puntuación de coincidencia R es mayor que un umbral preseleccionado para este modelo de usuario. El Motor de Autenticación e Identificación 130, el Motor de Construcción de Modelos 155 y la Base de datos de Modelos de Usuario 135 forman una unidad AID 160.

La Firma 125 también se alimenta al Motor de Construcción de Modelos 155 para inicializar el modelo de usuario durante la primera vez que se inscribe o incorpora selectivamente la información de la firma para refinar el modelo de usuario almacenado en la Base de datos de Modelos de Usuario 135 si el modelo ya está presente. En una realización de la presente invención, el Motor de Construcción de Modelos 155 actualiza las medias y varianzas Mi y Vi mencionados anteriormente usando la firma extraída de nuevas imágenes del usuario.

El Dispositivo 100 también contiene preferiblemente una Interfaz de Recursos Remotos 145, que se comunica con el Motor AID 130. La Interfaz de Recursos Remotos 145 sirve como interfaz entre las funcionalidades de autenticación e identificación implementadas en el Dispositivo 100 y esas mismas funcionalidades que ocurren en recursos externos/remotos, tales como servidores remotos y dispositivos remotos. Así, por ejemplo, la Interfaz de Recursos Remotos 145 interactúa con aplicaciones residentes en servidores remotos para coordinar la autenticación o identificación según lo requieran las aplicaciones remotas. Esto puede incluir gestionar y responder a solicitudes de recursos externos para la autenticación o identificación de un usuario que opera el Dispositivo 100 o para la autenticación o identificación del Dispositivo 100 en sí mismo.

La Interfaz de Recursos Remotos 145 puede comunicarse con la Interfaz de Red 150 para transmitir y recibir datos en relación con las actividades de autenticación e identificación. Se pueden utilizar diversos protocolos de comunicación inalámbrica, incluida la radiofrecuencia, así como otros, incluidos, y sin limitación, Bluetooth y otras tecnologías de

comunicaciones de campo cercano. En una realización preferida de la presente invención, los datos comunicados de un lado a otro desde el Dispositivo 100 a través del enlace inalámbrico abierto se aseguran como se conoce en la técnica mediante, por ejemplo, encriptación y/u otras metodologías, que reducen o eliminan el posibilidad de que los datos del usuario y otros datos asociados con las metodologías de autenticación e identificación de la presente invención puedan ser interceptados por partes no autorizadas. La Interfaz de Red 150 típicamente comprende un módulo transceptor de radiofrecuencia como se conoce en la técnica y permite que el Dispositivo 100 se comunique a través de un enlace inalámbrico con la Red Inalámbrica 400. La Red Inalámbrica 400, a su vez, típicamente hace retroceder los datos que son transmitidos por o para ser recibidos por Dispositivo 100 a la Red de Datos 500, nuevamente como se conoce en la técnica.

Solo a manera de ejemplo, la presente invención permite a los usuarios del Dispositivo 100 o el Dispositivo 100 en sí mismo autenticarse o identificarse mediante servidores remotos y aplicaciones y otros recursos que residen en servidores remotos. Como se ilustra en la Figura 1, el Servidor Remoto 200 puede comunicarse con el Dispositivo 100 a través de la ruta de comunicación discutida anteriormente. De esta manera y según lo controlado por la Interfaz de Recursos Remotos 145 que reside en el Dispositivo 100, la Unidad AID 205 que reside en el Servidor Remoto 200 puede solicitar y recibir datos de autenticación e identificación del Dispositivo 100 para compararlos con modelos de usuarios conocidos y validados que residen en o son accesibles por el Servidor Remoto 200 como se describe más detalladamente a continuación. Esta capacidad de autenticación e identificación proporciona acceso selectivo a una o más Aplicaciones 210, Datos 215 y otros recursos que residen en el Servidor Remoto 200. La misma capacidad también puede proporcionar acceso selectivo a los Recursos Locales 140, incluidas aplicaciones, datos y/o otros recursos que residen en el Dispositivo 100, así como en los casos en que tales recursos locales buscan acceso a datos u otros recursos que son remotos al Dispositivo 100.

En otra realización de la presente invención, la comunicación como se discutió anteriormente puede ocurrir entre el Dispositivo 100 y uno o más Dispositivos Remotos 300. Los Dispositivos Remotos 300 pueden ser los mismos o diferentes tipos de dispositivos que el Dispositivo 100 y la funcionalidad de autenticación/identificación de acuerdo con las enseñanzas de la presente invención puede ocurrir en ambos sentidos. En otras palabras, el Dispositivo 100 puede responder a las solicitudes de autenticación/identificación del Dispositivo Remoto 300 para acceder, por ejemplo, a una o más Aplicaciones 310 y/o Datos 315 que residen en el Dispositivo Remoto 300 a través de la Unidad AID 305 en el Dispositivo Remoto 300. Pero también, el Dispositivo Remoto 300 puede recibir y responder a las solicitudes de autenticación e identificación iniciadas por el Dispositivo 100 con el fin de que el Dispositivo Remoto 300 (o un usuario que lo opera) acceda a los recursos residentes en el Dispositivo 100. En algunos casos, tanto el Dispositivo 100 como el Dispositivo Remoto 300 requerirá autenticación y/o identificación del otro antes de compartir los recursos. Esto puede ocurrir, por ejemplo, en el contexto de una comunicación segura deseada entre los usuarios del Dispositivo 100 y el Dispositivo Remoto 300.

Volviendo ahora a la Figura 2, se describe a continuación la metodología de autenticación y/o identificación de usuario/dispositivo de acuerdo con una realización preferida de la presente invención. A modo de discusión inicial, se describe primero la diferencia entre autenticación e identificación en el contexto de las enseñanzas de la presente invención.

En el caso de la autenticación, el usuario presenta una identidad en forma de una ID de usuario o nombre de usuario y el sistema de la presente invención verifica que el usuario es realmente quien dice ser. Luego, el sistema compara la firma derivada de una imagen o imágenes de la palma del usuario con el modelo correspondiente en la base de datos de modelos de usuario. Si coinciden, el usuario se autentica. Si no coinciden, el usuario es rechazado.

El diagrama de flujo para la autenticación de usuario de acuerdo con las enseñanzas de la presente invención, en una realización preferida, se muestra en la Figura 4. Como primera etapa, el usuario en el Dispositivo 100 puede ingresar su nombre u otra información de identificación en el Dispositivo 100, o la identidad del usuario ya puede estar precargada en el Dispositivo 100. Por separado, el usuario toma una imagen o un conjunto de imágenes de la palma de su mano o manos usando la Cámara 105 del Dispositivo 100. A continuación, el Procesador de Datos de Cámara 110 envía los datos de píxeles sin procesar al Detector de Región de Interés 115 el cual determina el área de la palma dentro de la imagen. El área de la palma enmascarada del Detector de Región de Interés 115 se alimenta al Procesador de Conversión 120, el cual deriva la firma única del usuario. Esta función de conversión puede procesarse alternativamente en un recurso remoto o parcialmente en un recurso remoto y parcialmente en el Dispositivo 100. Sin contacto directo entre el área de la palma de la imagen y el Dispositivo 100, utilizando imágenes de alta resolución de la mano, tomadas en forma libre y en cualquier orientación por parte del usuario final sin ningún hardware especial más allá de una cámara digital común, el sistema de la presente invención identifica al individuo utilizando una solución de software multietapas que involucra extracción de características, procesamiento de características en firmas de usuario y la coincidencia de firmas de usuario con firmas de usuario almacenadas o modelos de usuario en los que: (i) se detectan y segmentan una o varias regiones de interés de la imagen de entrada para eliminar datos de píxeles extraños y aislar el área de la palma; (ii) se extraen de la imagen un número de vectores de características dispersas de alta dimensión (véase, por ejemplo, la referencia 8); (iii) se crea una única firma para cada imagen en un proceso en el que los vectores de características cercanos se agrupan en una representación de imagen más compacta y robusta; y (iv) múltiples firmas de imágenes se combinan en un modelo de identidad para cada usuario individual.

El Motor de Autenticación e Identificación 130 luego busca el modelo del usuario (basado en los datos de identificación del usuario presentados previamente) en la Base de datos de Modelos de Usuario 135. En este punto, si la firma del usuario derivada coincide con el modelo de usuario almacenado, el usuario se autentica y se permite el acceso al recurso o conjunto de recursos deseado. Alternativamente, si la firma y el modelo del usuario no coinciden, entonces se le denegará al usuario el acceso al recurso o conjunto de recursos deseado. La funcionalidad anterior con respecto a la búsqueda y la coincidencia puede realizarse alternativamente de forma remota al Dispositivo 100.

En caso de identificación, el usuario presenta solo una imagen de huella de la palma o un conjunto de imágenes, y el Motor de Autenticación e Identificación 130 compara la firma derivada de la imagen o imágenes de huella de la palma con todos los modelos o un subconjunto de modelos en la Base de datos de Modelos de Usuario 135. Si se encuentra una coincidencia, entonces el usuario es identificado. Si no se encuentra ninguna coincidencia, el usuario es desconocido.

El diagrama de flujo para la identificación del usuario se muestra en la Figura 5. En este caso, como en el caso de la autenticación, el usuario toma una fotografía o un conjunto de fotografías de la palma de su mano. Estos datos son procesados nuevamente en forma de píxeles por el Procesador de Datos de Cámara 110 y enviados al Detector de Región de Interés 115 para determinar el área de la palma dentro de la imagen. El área de la palma enmascarada del Detector de Región de Interés 115 se alimenta al Procesador de Conversión 120, lo cual deriva la firma única del usuario y luego el Motor AID 130 compara la firma derivada con todos los modelos o un subconjunto de modelos almacenados en la Base de datos de Modelos de Usuario 135. Las funciones de conversión y comparación mencionadas anteriormente podrían procesarse alternativamente en un recurso remoto o parcialmente en un recurso remoto y parcialmente en el Dispositivo 100. En cualquier caso, si se encuentra una coincidencia, entonces el usuario es identificado y se le puede otorgar acceso a un recurso o conjunto de recursos. Si no se encuentra ninguna coincidencia, el usuario no puede ser identificado y no se otorgará acceso al recurso o conjunto de recursos deseado.

El modo (autenticación o identificación) utilizado depende de la aplicación. En general, la autenticación proporciona un mayor grado de precisión, pero un menor nivel de experiencia del usuario debido a la etapa adicional que un usuario debe tomar para ingresar un factor adicional de su identidad. El segundo factor de identidad puede tomar cualquiera de las formas comunes, tales como un nombre de usuario, ID de usuario, contraseña, ID de empleado único, número de seguro social, dirección de correo electrónico, una variedad de otras modalidades biométricas, entre otras. En una realización de la presente invención, el segundo factor de identidad es la firma derivada de las imágenes de huella de la palma de la segunda mano del individuo, con las firmas individuales de cada una de las imágenes o conjuntos de imágenes de la palma del individuo utilizadas en conjunto para autenticación o identificación.

Es importante tener en cuenta que en cada caso descrito anteriormente (autenticación o identificación), en lugar de comparar una firma de usuario con un modelo dentro de la Base de datos de Modelos de Usuario 135 localmente ubicada dentro del Dispositivo 100, una firma generada por una imagen o conjunto de imágenes de una palma del usuario tomada en el Dispositivo 100 podría coincidir con un modelo o modelos contenidos en una base de datos ubicada en uno o ambos del Servidor Remoto 200 o uno o más Dispositivos Remotos 300. En este caso, el usuario del Dispositivo 100 típicamente buscaría acceso a uno o más recursos residentes en estas plataformas remotas en lugar de un recurso ubicado localmente dentro del Dispositivo 100. A modo de ejemplo, en el caso de desbloquear, por ejemplo, un teléfono inteligente, el procesamiento podría realizarse localmente en el teléfono inteligente/Dispositivo 100, mientras que si la autenticación se está llevando a cabo, por ejemplo, en relación con una aplicación con base remota, alguna porción del procesamiento podría realizarse en un Servidor Remoto 200 con modelos de usuario para compararlos con el posible almacenamiento en el Servidor Remoto 200 en lugar de localmente en el teléfono inteligente. Además, debería ser evidente a partir de las enseñanzas actuales que los modelos de usuario, las firmas y/u otros datos biométricos pueden sincronizarse entre cualquiera de las Unidades AID 160, 205, 305 para permitir la autenticación o identificación local en uno cualquiera de los Dispositivos 100, Servidor Remoto 200, Dispositivo Remoto 300 sin dicho Dispositivo 100, el Servidor Remoto 200 o el Dispositivo Remoto 300 han generado ese modelo de usuario, firma y/u otros datos biométricos localmente.

Volviendo ahora a la Figura 2, se puede ver que en una realización preferida de la presente invención, en la etapa (1), el Dispositivo 100 se usa para tomar una imagen o serie de imágenes de la palma del usuario a identificar (etapa (2)) con la Cámara 105 (etapa (3)). Se puede integrar un componente de *flash* (etapa (4)) en el Dispositivo 100 para proporcionar el preprocesamiento necesario de la imagen, particularmente en lo que se refiere a proporcionar una luz mínima suficiente para la detección de la región de interés, la extracción de características y el procesamiento de la firma de la imagen de la palma del individuo. A continuación, la región de la palma de la imagen se enmascara mediante el Detector de Región de Interés 115 (etapa (5)) y se alimenta al Procesador de Conversión 120 (etapa (6)) para convertir píxeles sin procesar en una firma de usuario de identificación única, la Firma 125. La firma de usuario es un código compacto que contiene información de identificación relevante asociada con la imagen de huella de la palma del usuario y puede coincidir de manera rápida y precisa con una gran base de datos de modelos de usuario tal como la Base de datos de Modelos de Usuario 135 o una base de datos en una plataforma remota (etapa (7)) Un beneficio de la firma de usuario derivada es que hace que sea esencialmente imposible reconstruir la imagen de la palma de un usuario a partir de una base de datos de modelos de usuario. En la etapa (8), el Motor AID 130 compara la firma de usuario a partir de la imagen de la palma o el conjunto de imágenes con las de la base de datos de modelos de usuario para identificar o autenticar al usuario según corresponda. Las funciones de conversión y comparación mencionadas

anteriormente podrían procesarse alternativamente en un recurso remoto o parcialmente en un recurso remoto y parcialmente en el Dispositivo 100.

Volviendo ahora a la Figura 3, se puede ver que en los casos en que se realiza la autenticación o identificación con respecto a un recurso remoto, la comunicación entre el Dispositivo 100 y ese recurso remoto se produce preferiblemente a través de una conexión segura como se conoce en la técnica. Esto puede implicar una o más técnicas, como se sabe en la técnica, que incluyen, por ejemplo, encriptación segura, encriptación de clave pública o privada, certificados digitales y/o firmas digitales, entre otras.

Ahora que se han descrito el sistema y las metodologías principales de la presente invención, se discutirán novedosas características adicionales, tales como diversas metodologías para evitar la suplantación de identidad en relación con la autenticación/identificación, así como una novedosa metodología para codificar e intercambiar información de transacciones con recursos remotos.

La protección contra la suplantación es un aspecto importante de esta invención. Evita que los adversarios, por ejemplo, usen una fotografía impresa de una palma en lugar de una mano real para la autenticación. Un aspecto novedoso de la presente invención que está dirigida a la protección contra la suplantación implica detectar y usar las características tridimensionales de una mano humana para proporcionar seguridad contra la suplantación de identidad.

En un ejemplo de detección de suplantación, para distinguir entre una fotografía y una mano real, el sistema de la presente invención toma una serie de imágenes en secuencia rápida, utilizando el *flash* de la cámara de manera intermitente y en diferentes períodos de tiempo. Las imágenes de un objeto tridimensional (una mano real) tomadas con el *flash* tendrán ciertas regiones resaltadas y sombras creadas por el *flash*, mientras que en las posiciones de la mano en las que una representación bidimensional de la mano (por ejemplo, un la fotografía impresa de una palma o una imagen de la palma que se muestra en la pantalla de visualización de otro dispositivo móvil) no mostraría tales regiones y sombras resaltadas. Esto permite que el sistema de la presente invención utilice una comparación de las regiones y sombras resaltadas en la mano creada entre las fotos con *flash* y sin *flash* para distinguir entre una fotografía impresa y una mano real. De esta manera, una parte no autorizada que haya obtenido una imagen de la palma de un usuario autorizado no puede usar esa imagen para obtener acceso no autorizado a recursos locales o remotos.

Métodos adicionales para detectar una mano real incluyen el modelado tridimensional de la mano. En este caso, el sistema de la presente invención puede incitar al usuario a girar la mano mientras se toman una serie de imágenes múltiples. Un verdadero objeto 3-D revelará diferentes partes de la mano con cada imagen sucesiva, mientras que un objeto 2-D siempre mostrará exactamente la misma parte de la mano, solo con diferentes grados de distorsión. Esto permite que el sistema de la presente invención distinga entre una fotografía impresa y una mano real. Del mismo modo, en lugar de girar la mano, se le puede solicitar al usuario que cierre la mano en puño o que la abra desde el puño mientras se toma la serie de imágenes. También son posibles otros métodos para distinguir una mano real de la fotografía de una mano.

Otro aspecto novedoso de la presente invención es una metodología en la que se pueden detectar y prevenir ataques de repetición. En este caso, un adversario modifica un dispositivo móvil de modo que envía una o una serie de imágenes grabadas previamente de la mano real de un usuario legítimo a la red para autenticación o identificación en lugar de enviar las imágenes tomadas por la cámara. Aquí se supone que el adversario podría tomar fotografías de la mano de un usuario autorizado sin que el usuario autorizado sea consciente o pueda evitarlo. Si esto es de hecho un riesgo (por ejemplo, un caso en el que un usuario autorizado está durmiendo o inconsciente), entonces es preferible para el sistema que se use de tal manera que se requieran uno o más factores de identidad adicionales, tales como ID de usuario u otra forma de datos independiente de la imagen de huella de la palma para autenticar a un usuario.

Para detectar y defenderse contra un ataque de repetición, el sistema de la presente invención emite una serie de imágenes y *flash*es en una variedad de intervalos, es decir, graba una serie de imágenes, algunas con el *flash* apagado y otras con el *flash* encendido. Las imágenes específicas y la secuencia de encendido/apagado del *flash* se pueden elegir al azar o de acuerdo con una secuencia predeterminada y pueden cambiar para cada solicitud de autenticación o identificación. El sistema de la presente invención puede detectar fácilmente si un adversario usa una serie de imágenes previamente grabadas porque el patrón de activación/desactivación de las imágenes y los *flash*es no coincidirán con el que realmente se envió al dispositivo móvil.

Otro método para detectar un ataque de repetición implica almacenar todas las imágenes utilizadas anteriormente y comparar nuevas imágenes con esa base de datos. Debido a que los datos de píxeles subyacentes a las imágenes de dos palmas diferentes nunca pueden ser exactamente iguales o sustancialmente iguales a un cierto nivel de tolerancia, el sistema puede detectar cuándo se usa nuevamente una imagen tomada previamente. También son concebibles otros métodos para detectar un ataque de repetición.

Otro aspecto novedoso de la presente invención es la capacidad de integrar información de transacciones u otros datos dentro del tiempo de una serie de fotografías y/o patrones de *flash*. Este patrón de tiempo se puede utilizar además para codificar información sobre la transacción en sí misma. Entonces se puede aplicar un código de direccionamiento criptográfico a esta información. El código de direccionamiento hace que el código resultante sea compacto (corto) y también evita que cualquier persona que observe el patrón *flash* obtenga información sobre el

contenido original del código. En una realización de la presente invención, la sincronización de la secuencia de imágenes y/o patrones de *flash* se utiliza como parte de un mecanismo antisuplantación de identidad para determinar si la secuencia de imágenes proporcionada para autenticación o identificación coincide con la información de la transacción misma. Una implementación específica puede incluir:

1. Un vídeo de baja resolución del área de la palma con los patrones de flash.

2. Una o varias imágenes fijas de alta resolución del área de la palma.

3. Tecnología de visión por ordenador para garantizar que las imágenes de alta resolución provengan del mismo objeto que las del vídeo.

Con base en la descripción anterior del sistema y las metodologías de la presente invención, se puede entender que son posibles diversas aplicaciones. Ejemplos incluyen, sin limitación, acceso a uno o más dispositivos, acceso a una o más aplicaciones residentes en esos dispositivos o ubicadas de forma remota en un servidor u otros dispositivos remotos, una variedad de aplicaciones transaccionales (tales como votación electoral, distribución de beneficios sociales del Estado), pagos financieros) y cualquier otro tipo de transacción que requiera la validación de la identidad del usuario.

En resumen, en realizaciones de ejemplo, la presente invención proporciona sistemas informáticos (que incluyen una combinación de software que se ejecuta en hardware adecuado), métodos implementados por ordenador y dispositivos para autenticación o identificación de un individuo que incluye el uso de una imagen o un conjunto de imágenes de la palma de una persona a través de un proceso que involucra las siguientes etapas: (1) detectar el área de la palma usando clasificadores locales; (2) extraer características de las regiones de interés; y (3) calcular el puntaje de coincidencia contra modelos de usuario almacenados en una base de datos, que pueden aumentarse dinámicamente a través de un proceso de aprendizaje. Por lo tanto, la invención incluye un sistema para proporcionar acceso selectivo a los recursos disponibles en conexión con un dispositivo que comprende software ejecutado en hardware informático adecuado, en el que el sistema comprende: (a) al menos una cámara asociada con dicho dispositivo, siendo dicha cámara capaz de tomar al menos una fotografía de una huella de la palma humana; (b) un módulo detector que utiliza clasificadores locales para localizar y segmentar la región de interés de la palma sin contacto físico; (c) un procesador de conversión que convierte los datos de píxeles sin procesar asociados con dicha región de interés de una huella de la palma humana en una firma única asociada con dicha huella de la palma; y (d) un motor de autenticación e identificación, determinando dicho motor de autenticación e identificación si el acceso a uno o más de dichos recursos debe otorgarse con base en dicha firma única y al menos una base de datos que contiene una pluralidad de modelos de usuario. El sistema puede comprender además un procesador de aprendizaje que mejora los modelos de usuario con nuevos datos, en el que el procesador de aprendizaje incluye selectivamente dicha imagen de huella de la palma para aumentar dicha base de datos y dicho motor de autenticación e identificación. En realizaciones, el dispositivo es un dispositivo móvil, mientras que en otras realizaciones, el dispositivo es un dispositivo de escritorio o un dispositivo integrado estacionario. El sistema puede incluir un componente de *flash* que se activa selectivamente en el momento de la captura de imágenes para proporcionar luz mínima suficiente para la detección de la región de interés, la extracción de características y el procesamiento de firma de la imagen de la palma de humano. En realizaciones, el procesador de conversión del sistema usa descriptores extraídos de parches sobre la región de interés. Los descriptores se pueden codificar en vectores dispersos de alta dimensión, que se pueden agrupar en al menos un grupo.

El sistema de la invención puede tener, como parte del método implementado dentro del sistema, la característica de calcular una firma de una Bolsa de Características o múltiples representaciones de Bolsas de Características. Además, el módulo detector del sistema puede usar los algoritmos Haar Wavelets y AdaBoost. En diversas realizaciones, el sistema incluye un módulo detector que utiliza máquinas de vectores de soporte o una red neuronal convolucional. El módulo de usuario del sistema puede ser un modelo estadístico calculado a partir de una colección de imágenes de la palma de un humano. Del mismo modo, el modelo de usuario puede ser un modelo de densidad gaussiana o una mezcla de modelo de densidad gaussiana.

El sistema de la invención puede configurarse de tal manera que al menos uno de los recursos esté alejado del dispositivo. Alternativamente, al menos uno de los recursos puede residir en el dispositivo. En algunas realizaciones, al menos uno de los recursos es una aplicación o una base de datos.

En realizaciones del sistema de la invención, las firmas individuales de cada una de las dos imágenes de huella de la palma de un humano, si están disponibles, se utilizan en conjunto para la autenticación o identificación del humano.

En algunas realizaciones del sistema de la invención, la autenticación o identificación de huellas de la palmas se combina con otras modalidades, tales como una o más de las siguientes: claves de acceso, preguntas de seguridad, reconocimiento de huellas digitales, reconocimiento facial, reconocimiento de iris, reconocimiento de firma escrita y otras modalidades biométricas y no biométricas.

El sistema de la invención puede implementarse de tal manera que una aplicación permita selectivamente que uno o más usuarios realicen una o más transacciones.

El sistema de la invención también puede incluir el uso de una secuencia de imágenes con *flash* y sin *flash* de la palma de la mano de un humano, que se pueden usar, entre otras cosas, como parte de un mecanismo antisuplantación para determinar si la mano presentada es objeto tridimensional o una representación bidimensional de una mano. Además, el sistema de la invención puede implementarse de tal manera que los datos de imagen capturados durante el movimiento de la palma del humano se utilicen como parte de un mecanismo antisuplantación para determinar si la mano presentada es un objeto en representación 3-D o en 2-D de una mano. En algunas realizaciones, la secuencia de imágenes *flash* y no *flash* de la palma del humano, así como los intervalos de tiempo entre imágenes sucesivas, se utilizan como parte de un mecanismo antisuplantación para determinar si un adversario está intentando utilizar una secuencia previamente grabada de imágenes para autenticación o identificación.

En algunas realizaciones de la invención, todas las imágenes previamente utilizadas de un humano se almacenan, tal como en una base de datos residente en un dispositivo informático, para compararlas contra nuevas imágenes como parte de un mecanismo antisuplantación para determinar si un adversario está intentando utilizar imágenes previamente grabadas para autenticación o identificación. Y aún además, en ciertas realizaciones, el sistema de la invención se implementa de tal manera que la información de la transacción u otros datos se integran dentro del tiempo de una secuencia de imágenes y/o patrones de *flash* como parte de un mecanismo antisuplantación para determinar si la secuencia de imagen proporcionada para la autenticación o identificación coincide con la información de la transacción misma.

Si bien se han mostrado y descrito realizaciones particulares de la presente invención, será obvio para los expertos en la técnica que, basándose en las enseñanzas de la presente, se pueden hacer cambios y modificaciones sin apartarse de esta invención y sus aspectos más amplios.

Referencias citadas

(1) Paul Viola and Michael Jones, Rapid Object Detection using a Boosted Cascade of Simple Features, Proceedings of IEEE Computer Vision and Pattern Recognition, 2001, pages 1:511-518.

(2) Corinna Cortes and Vladimir N.Vapnik, Support-Vector Networks, Machine Learning, 20, 1995.

(3) Yann LeCun, Léon Bottou, Yoshua Bengio, Patrick Haffner: Gradient-Based Learning Applied to Document Recognition, Proceedings of the IEEE, 86(11):2278-2324, November 1998.

(4) Pierre Sermanet, Koray Kavukcuoglu, Soumith Chintala and Yann LeCun: Pedestrian Detection with Unsupervised Multi-Stage Feature Learning, Proc. International Conference on Computer Vision and Pattern Recognition (CVPR'13), IEEE, June 2013.

(5) David G. Lowe, "Distinctive image features from scale-invariant keypoints," International Journal of Computer Vision, 60, 2 (2004), pp. 91-110.

(6) N. Dalal and B. Triggs. Histograms of oriented gradients for human detection. In Proceedings of Computer Vision and Pattern Recognition, 2005.

(7) Y-Lan Boureau, Jean Ponce and Yann LeCun: A theoretical analysis of feature pooling in vision algorithms, Proc. International Conference on Machine learning (ICML'10), 2010.

(8) Yann LeCun, Koray Kavukvuoglu and Clément Farabet: Convolutional Networks and Applications in Vision, Proc. International Symposium on Circuits and Systems (ISCAS'10), IEEE, 2010.

REIVINDICACIONES

1. Un sistema antisuplantación para detectar y usar características tridimensionales de una huella de la palma humana con el fin de proporcionar acceso selectivo a los recursos disponibles en conexión con un teléfono inteligente basado en un método de aprendizaje, comprendiendo el sistema:

(a) un teléfono inteligente que comprende un procesador digital, un módulo de memoria, un sistema operativo y medios de almacenamiento no transitorios que comprenden instrucciones ejecutables por el procesador digital;

(b) al menos una cámara asociada con el teléfono inteligente y configurada para capturar una pluralidad de imágenes que comprenden una imagen con *flash* y una imagen sin *flash* de una huella de la palma humana de un primer usuario, en donde la pluralidad de imágenes se captura sin que la palma humana toque físicamente el teléfono inteligente; y

(c) al menos un componente de *flash* asociado con el teléfono inteligente y configurado para emitir un *flash* durante la captura de la imagen con *flash* y no emitir un *flash* durante la captura de la imagen sin *flash*,

en donde el procesador digital está configurado para realizar lo siguiente:

(1) utilizar clasificadores locales basados en ventanas deslizantes y clasificadores formados por características locales discriminatorias aprendidas de una colección de imágenes de ejemplo para analizar la imagen con *flash* y la imagen sin *flash* de la huella de la palma humana para etiquetar los píxeles de la palma y los que no son de la palma mediante puntajes de clasificación;

(2) usar un detector para localizar y segmentar una región de interés de la huella de la palma humana dentro de la imagen con *flash* y la imagen sin *flash*;

(3) usar pequeñas ventanas de muestreo dentro de la región de interés para identificar parches de imágenes que abarcan rasgos biométricos característicos de la huella de la palma humana;

(4) extraer una firma de datos a nivel de píxel de los parches de imagen, en donde la firma es única para el primer usuario y se usa para distinguir al primer usuario de un segundo usuario, y en donde la extracción de la firma comprende crear un histograma de orientaciones de borde en una pluralidad de parches de imagen;

(5) determinar un intento de suplantación con base en una característica tridimensional de la huella de la palma humana y una pluralidad de modelos de usuario almacenados determinando si la imagen con *flash* representa un objeto tridimensional o una representación bidimensional de una palma humana, en donde la característica tridimensional se basa en una comparación entre la imagen con *flash* y la imagen sin *flash*, y en donde la comparación entre la imagen con *flash* y la imagen sin *flash* comprende determinar una región resaltada y una región de sombra en al menos una de la imagen con *flash* y la imagen sin *flash*;

(6) denegar el acceso a uno o más de los recursos al primer usuario, basado en la determinación del intento de suplantación de identidad; y

(7) almacenar al menos una de la pluralidad de imágenes de la huella de la palma humana y la característica tridimensional en la colección de imágenes de ejemplo.

2. El sistema antisuplantación de la reivindicación 1, en donde el procesador digital está configurado además para mejorar la pluralidad de modelos de usuario con nuevos datos incluyendo selectivamente al menos una imagen de la huella de la palma humana, los datos a nivel de píxel de parches de imagen y la firma para aumentar la al menos una base de datos y la determinación del intento de suplantación.

3. El sistema antisuplantación de la reivindicación 1 o la reivindicación 2, en donde el procesador digital está configurado además para funcionar usando descriptores extraídos de los parches de imagen sobre la región de interés, en donde los descriptores están codificados en vectores dispersos de alta dimensión, y en donde los vectores dispersos se agrupan en al menos un grupo.

4. El sistema antisuplantación de cualquiera de las reivindicaciones precedentes, en donde la firma se calcula a partir de una Bolsa de Características o múltiples representaciones de Bolsas de Características.

5. El sistema antisuplantación de cualquiera de las reivindicaciones precedentes, en donde el procesador digital, para analizar la imagen con *flash* y la imagen sin *flash* de la huella de la palma humana, está configurado además para funcionar usando uno o más de los siguientes: Algoritmos Haar Wavelets y AdaBoost, máquinas de vectores de soporte y una red neuronal convolucional; y los modelos de usuario comprenden uno o más de los siguientes: un modelo estadístico calculado a partir de una colección de imágenes de la palma humana del primer usuario, un modelo de densidad gaussiana y una mezcla de modelos de densidad gaussiana.

6. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde al menos uno de los recursos está alejado del teléfono inteligente, es residente en el teléfono inteligente, es una aplicación o es una base de datos.

7. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde las firmas individuales de ambas imágenes de huella de la palma de la mano del primer usuario se utilizan juntas para la determinación del intento de suplantación.

8. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde la denegación de acceso a uno o más de los recursos al primer usuario se combina con una o más otras modalidades biométricas, comprendiendo la una o más otras modalidades biométricas una o más más de lo siguiente: códigos de acceso, preguntas de seguridad, reconocimiento de huellas digitales, reconocimiento facial, reconocimiento de iris y reconocimiento de firma escrita.

9. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde denegar el acceso a uno o más de los recursos se basa además en denegar selectivamente a uno o más usuarios realizar una o más transacciones.

10. El sistema antisuplantación de cualquiera de las reivindicaciones precedentes, en donde al menos dos de la pluralidad de imágenes se capturan durante un movimiento de la palma humana, y en donde la característica tridimensional se basa además en el movimiento.

11. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde la pluralidad de imágenes comprende una secuencia de imágenes con *flash* e imágenes sin *flash*, y en donde la determinación del intento de suplantación se basa además en una comparación entre la secuencia de imágenes con *flash* y sin *flash* y una secuencia previamente grabada de imágenes con *flash* y sin *flash*.

12. El sistema antisuplantación de cualquiera de las reivindicaciones precedentes, en donde la determinación del intento de suplantación se basa además en una comparación entre al menos una de la pluralidad de imágenes y al menos una imagen de la primera huella de la palma del usuario en la colección de imágenes de ejemplo.

13. El sistema antisuplantación de la reivindicación 12, en donde una información de transacción u otros datos se integran dentro de uno o más intervalos de tiempo entre imágenes subsecuentes, y en donde la determinación del intento de suplantación se basa además en una comparación entre la información de la transacción y el transacción.

14. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde la captura de al menos una de la pluralidad de imágenes está separada de la captura de una imagen subsecuente por un intervalo de tiempo, y en donde la determinación del intento de suplantación está basado además en una comparación entre el intervalo de tiempo y un intervalo de tiempo anterior entre imágenes consecutivas previamente grabadas.

15. El sistema antisuplantación de una cualquiera de las reivindicaciones precedentes, en donde el sistema está configurado además para obtener en una serie de imágenes en secuencia rápida, con el *flash* de la cámara siendo usado de manera intermitente y en períodos de tiempo variables.

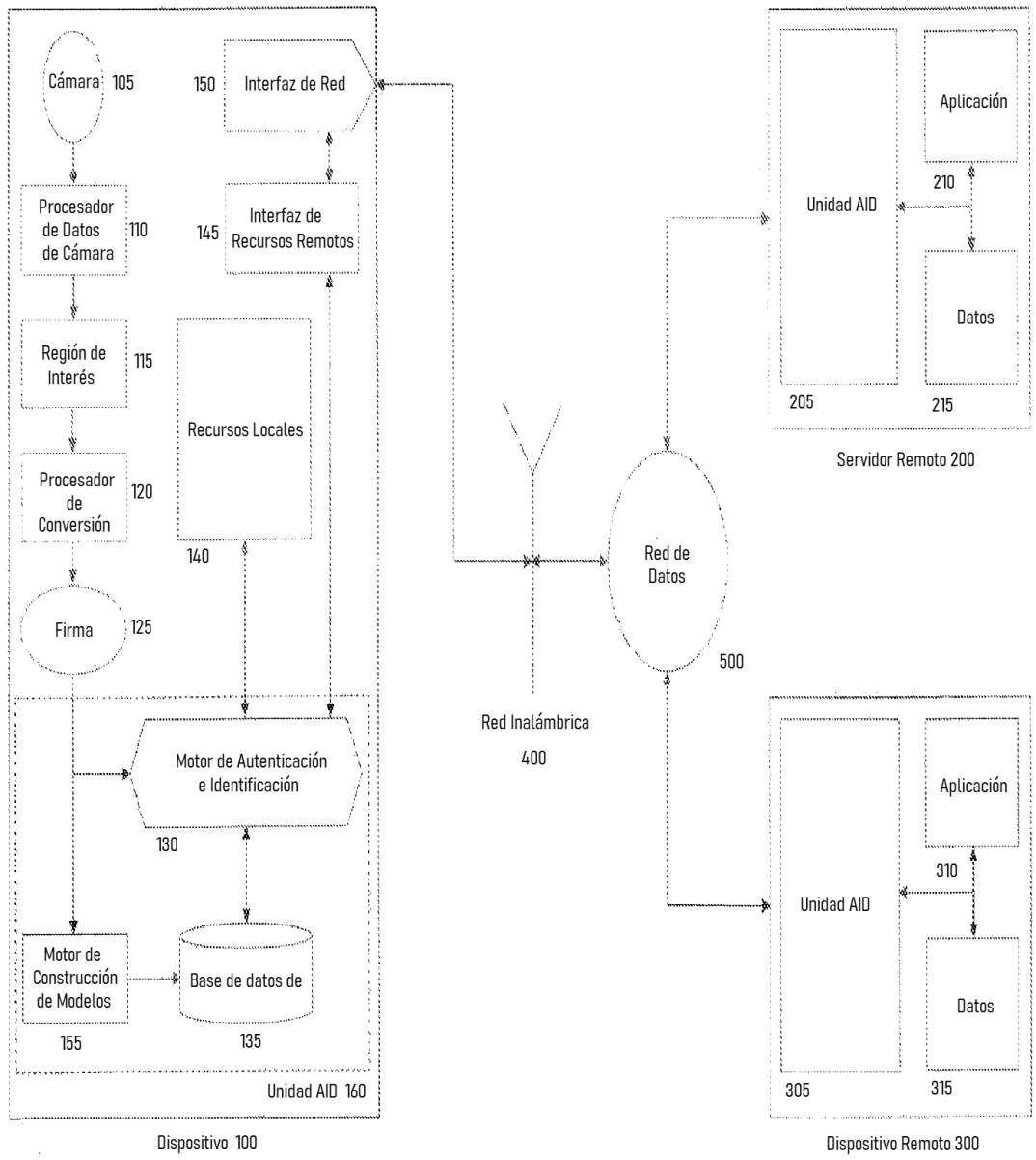
Cámara
105
150
Interfaz de Red
Procesador de Datos de Cámara
110
145
Interfaz de Recursos Remotos
Región de Interés
115
Recursos Locales
Procesador de Conversión
120
140
Firma
125
Motor de Autenticación e Identificación
130
Motor de Construcción de Modelos
155
Base de datos de
135
Unidad AID 160
Dispositivo 100
Red Inalámbrica
400
Red de Datos
500
Unidad AID
Aplicación
210
Datos
205
215
Servidor Remoto 200
Unidad AID
Aplicación
310
Datos
305
315
Dispositivo Remoto 300

FIGURA 1

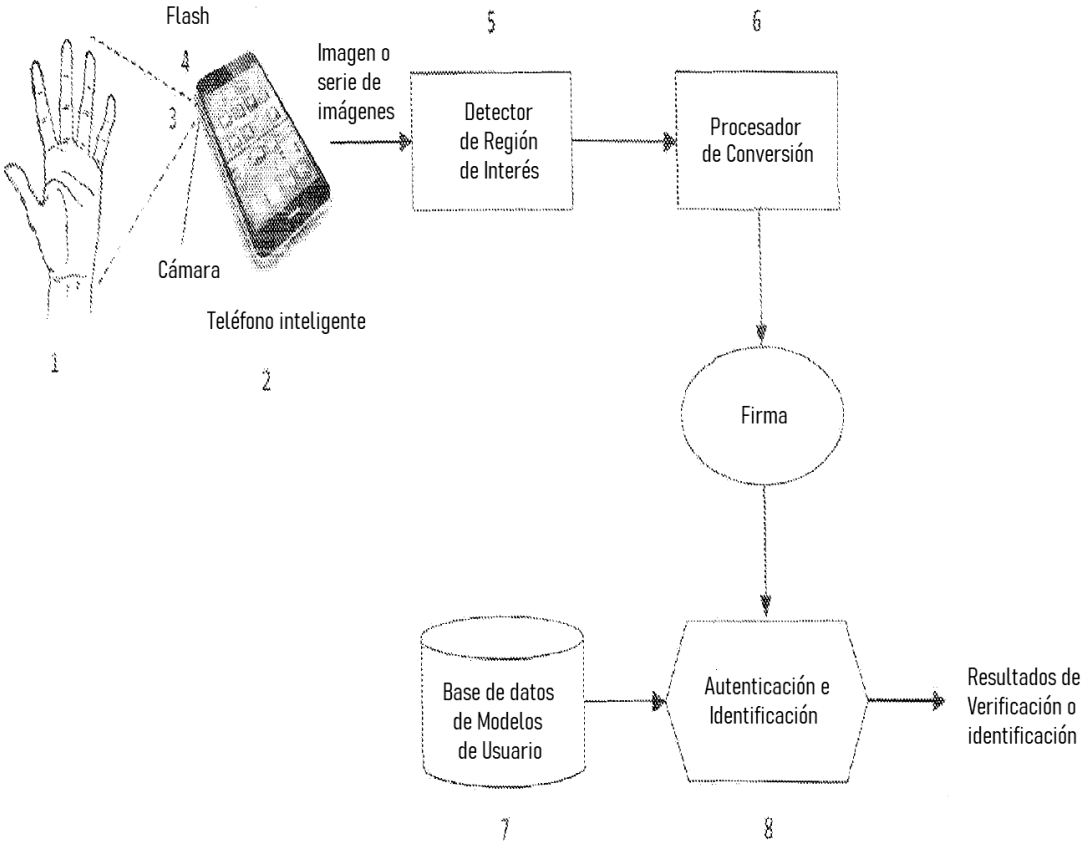
Flash
4
3
Cámara
Teléfono inteligente
2
1
Imagen o
serie de
imágenes
5
Detector
de Región
de Interés
6
Procesador
de Conversión
Firma
Base de datos
de Modelos
de Usuario
7
Autenticación e
Identificación
8
Resultados de
Verificación o
identificación

FIGURA 2

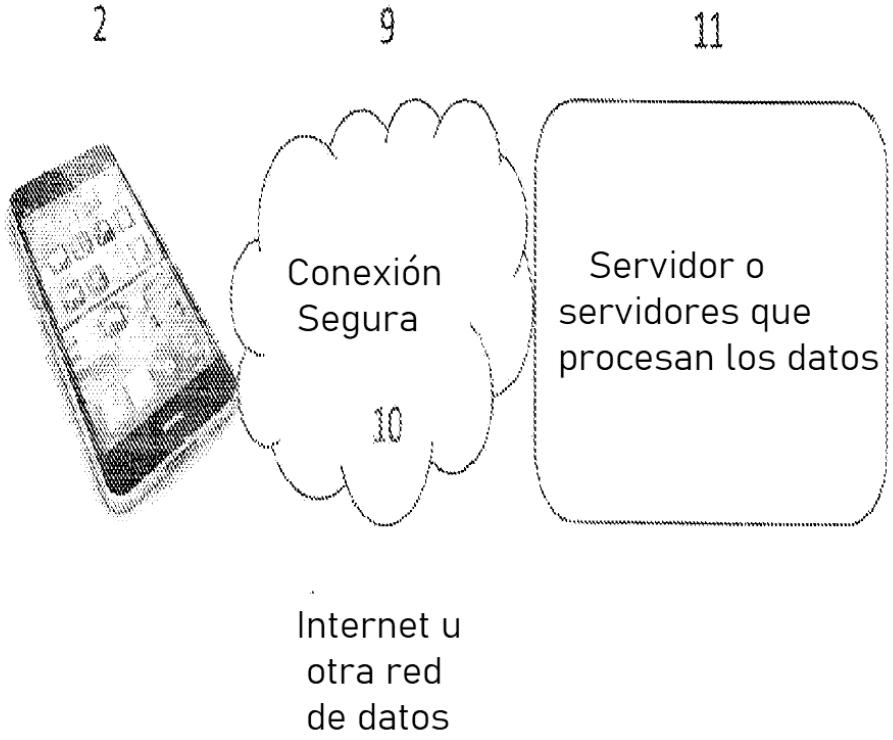
2
9
11
Conexión
Segura
10
Servidor o
servidores que
procesan los datos
Internet u
otra red
de datos

FIGURA 3

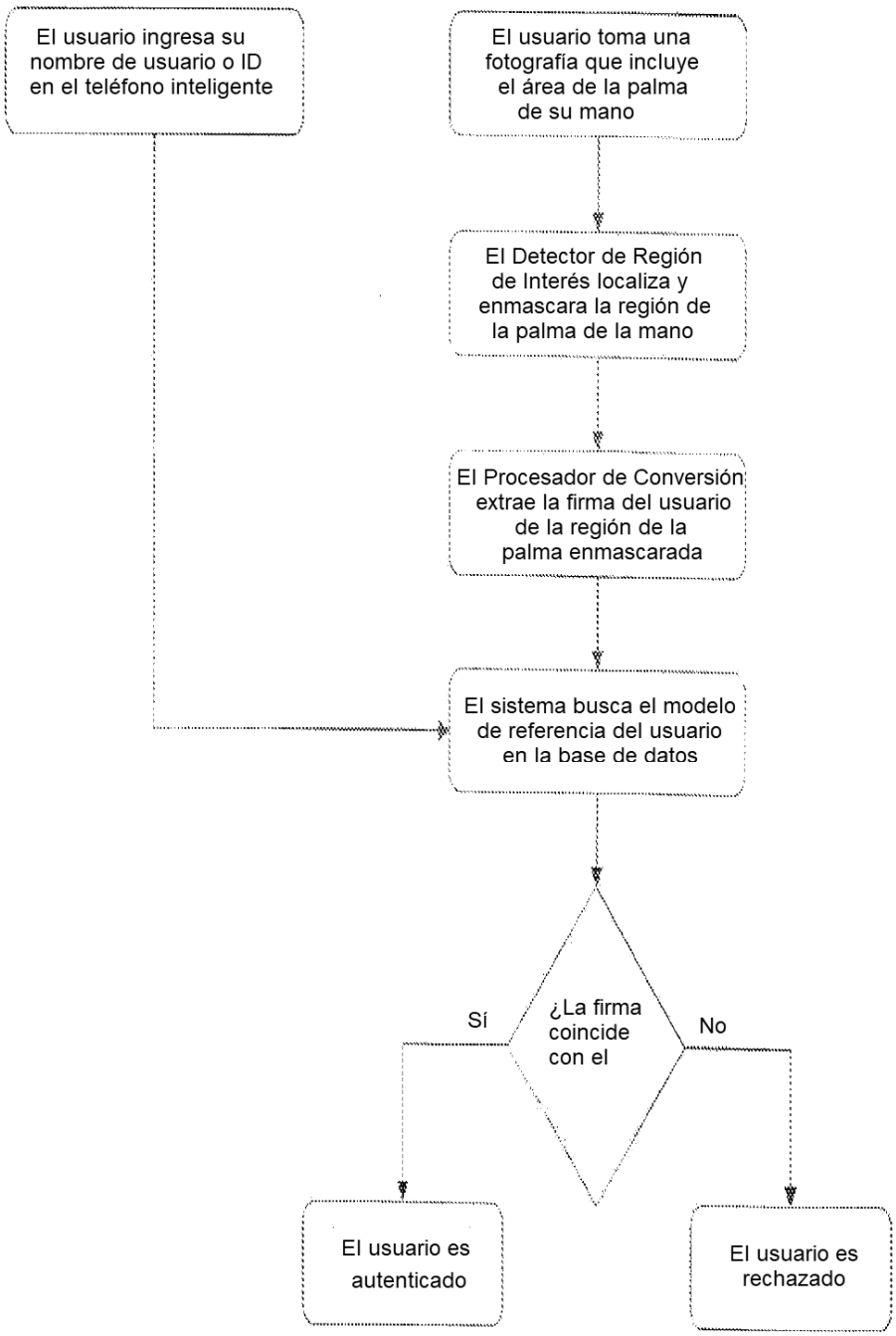
El usuario ingresa su nombre de usuario o ID en el teléfono inteligente
El usuario toma una fotografía que incluye el área de la palma de su mano
El Detector de Región de Interés localiza y enmascara la región de la palma de la mano
El Procesador de Conversión extrae la firma del usuario de la región de la palma enmascarada
El sistema busca el modelo de referencia del usuario en la base de datos
¿La firma coincide con el
Sí
No
El usuario es autenticado
El usuario es rechazado

FIGURA 4

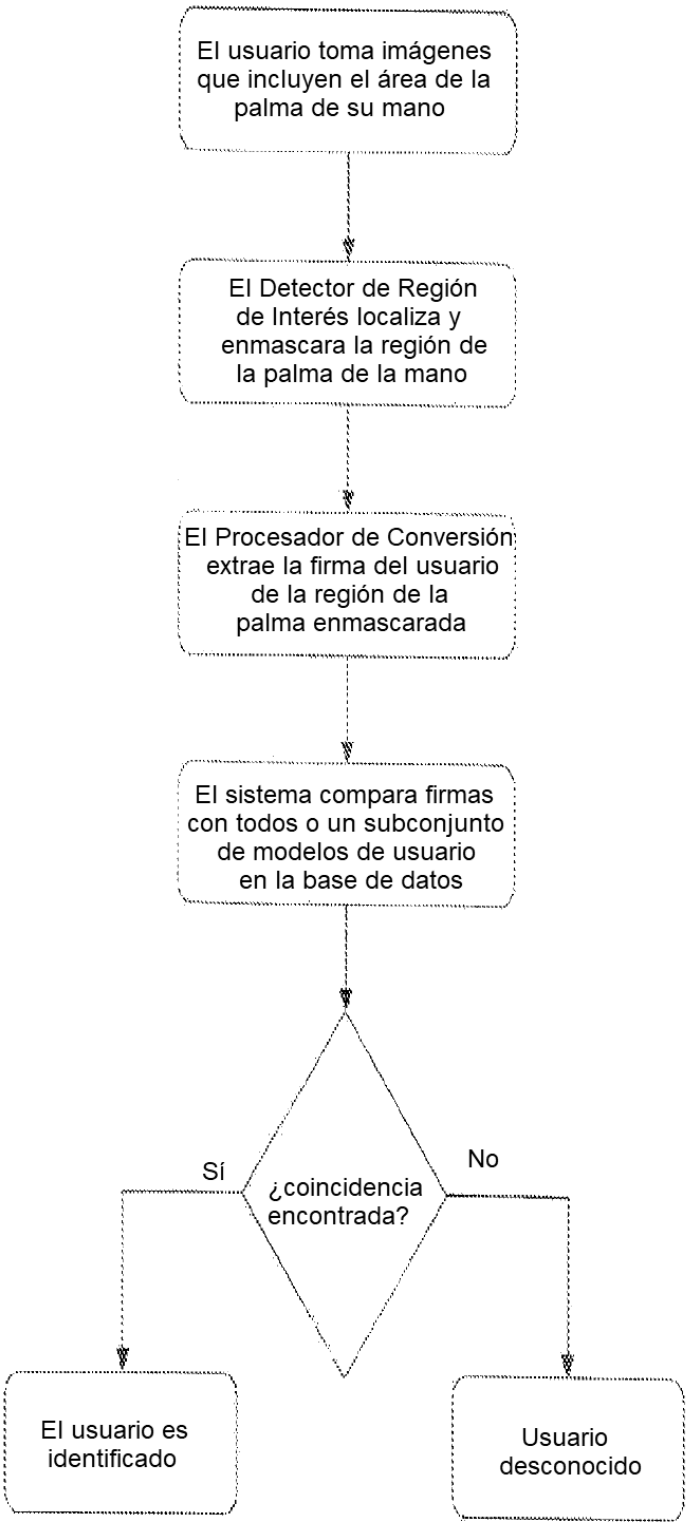
El usuario toma imágenes que incluyen el área de la palma de su mano
El Detector de Región de Interés localiza y enmascara la región de la palma de la mano
El Procesador de Conversión extrae la firma del usuario de la región de la palma enmascarada
El sistema compara firmas con todos o un subconjunto de modelos de usuario en la base de datos
¿coincidencia encontrada?
Sí
No
El usuario es identificado
Usuario desconocido

FIGURA 5