(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 813 876**

(51) Int. CI.:

G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.12.2014 PCT/EP2014/079460**

(87) Fecha y número de publicación internacional: **07.07.2016 WO16107651**

(96) Fecha de presentación y número de la solicitud europea: **30.12.2014 E 14828169 (4)**

(97) Fecha y número de publicación de la concesión europea: **15.07.2020 EP 3224757**

(54) Título: **Estructura de privacidad en un dispositivo para gafas inteligentes y relojes inteligentes**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.03.2021

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

HARIS MUGHEES, MUHAMMAD;
HUI, PAN y
PEYLO, CHRISTOPH

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Estructura de privacidad en un dispositivo para gafas inteligentes y relojes inteligentes

Campo técnico

La presente invención se refiere en general a una estructura para la privacidad en dispositivos inteligentes como gafas inteligentes o relojes inteligentes. En particular, la presente invención se refiere a un método para proporcionar una estructura para garantizar la privacidad de las personas que son detectadas por una cámara, preferiblemente una cámara digital de un dispositivo inteligente. La estructura de la presente invención puede ser proporcionada por un sistema y/o un método que garantice que esa privacidad de las personas en las fotos tomadas por la cámara del dispositivo inteligente es preservada, preferiblemente utilizando técnicas en el dispositivo. Preferiblemente, la estructura es implementada como software y/o hardware en el dispositivo inteligente.

Antecedentes de la Invención

Las gafas inteligentes son dispositivos informáticos portátiles en forma de anteojos computarizados, que típicamente comprenden un dispositivo de visualización óptico montado en la cabeza (OHMD). Debido a los últimos desarrollos en tecnología portátil, las gafas inteligentes modernas típicamente poseen una funcionalidad mejorada de procesamiento de datos similar a un teléfono inteligente o tableta y son capaces ejecutar aplicaciones sofisticadas (en lo sucesivo, también llamadas apps). Estos dispositivos también pueden incluir características especiales como superposición de realidad aumentada, GPS y capacidad de formación de mapas.

Otro dispositivo inteligente es un reloj inteligente (o reloj inteligente), que es un reloj de pulsera computarizado con una funcionalidad que es mejorada más allá de la precisión, y a menudo es comparable a un dispositivo de asistente digital personal (PDA). De manera similar a las gafas inteligentes, los relojes inteligentes ejecutan aplicaciones móviles y varios modelos ejecutan un sistema operativo móvil. Tales dispositivos pueden incluir características tales como una cámara, un teléfono móvil, pantalla táctil, navegación GPS, visualización de Mapas, etc.

A pesar de todas las ventajas, estos dispositivos inteligentes también dan lugar a nuevos desafíos acerca de la privacidad. Una característica principal con respecto a este aspecto es la cámara utilizada en estas gafas inteligentes. Dado que las gafas inteligentes son controladas por el usuario, el usuario puede controlar cuándo se toman fotos o videos, es decir, un usuario de forma típica no necesariamente solicitaría permiso a quienes lo rodean. Aunque cada usuario de un teléfono móvil o teléfono inteligente también puede tomar fotos y videos, en la mayoría de los casos es fácil reconocer cuándo el usuario está tomando una foto o un video, porque el usuario típicamente tiene que sostener el teléfono inteligente. Sin embargo, debido al tamaño y a la naturaleza de las gafas inteligentes, es mucho más difícil (si no imposible) reconocer cuándo un usuario está tomando una foto o un video con unas gafas inteligentes.

Además, las capacidades de reconocimiento facial pueden estar integradas fácilmente en gafas inteligentes. Por lo tanto, las fotos y videos de personas de la cámara en el dispositivo de las gafas inteligentes pueden ser identificadas con el software de reconocimiento facial. Una vez identificadas, el usuario de las gafas inteligentes podría ser presentado con el perfil de Facebook de la persona, el feed (“contenido sindicado”) de Twitter u otros resultados de búsqueda de Internet vinculados a su perfil. Típicamente, las personas no esperan una vinculación tan automatizada con sus datos de internet si se mueven en público, tienen una expectativa de anonimato.

Estos problemas de privacidad son graves y han llamado la atención a nivel oficial y personal. Por ejemplo, las "Google Glass ™" son conocidas en la técnica. El dispositivo es capaz de grabar audio, video, y fotos. Este dispositivo también puede utilizar GPS (Sistema de Posicionamiento Global) para el rastreo-ubicación y las direcciones. El dispositivo también es capaz de manejar tareas computacionales, ya que también está equipado con chip de procesador y GPU. Por ejemplo, existe una aplicación (“app”) para tomar subrepticiamente guiñando un ojo. Para un individuo externo, es difícil o imposible reconocer si el usuario de las gafas inteligentes está grabando audio o video con las gafas inteligentes. Además, todos los datos grabados por las gafas inteligentes, incluyendo fotos, videos, audio, datos de ubicación, y datos de usuario, pueden ser almacenados en un servidor en la nube, p. ej., en los servidores en la nube de Google. Las gafas inteligentes actuales pueden conectarse a Internet a través de Wi-Fi, o conectarse al teléfono inteligente del usuario. Además, incluso cuando están desconectadas temporalmente, las gafas inteligentes pueden grabar audio y/o video.

Recientemente, miembros del Congreso le solicitaron a un alto ejecutivo de Google Inc. que garantizara la protección de la privacidad de los dispositivos de gafas inteligentes. Además, una nueva encuesta de alrededor de 4.000 residentes del Reino Unido realizada por Rackspace y Goldsmiths en la Universidad de Londres descubrió que el 20 por ciento de los encuestados cree que las gafas inteligentes deberían ser prohibidas por completo, mientras que el 61 por ciento piensa que las gafas inteligentes y otros dispositivos de cámara portátiles deberían al menos ser regulados. Otra encuesta realizada por Bite Interactive muestra que solo el 10% de los residentes de EE.UU. confía en las gafas inteligentes. Además, muchos lugares de entretenimiento privados han prohibido las gafas inteligentes.

Ya existen algunos esfuerzos para cambiar la política de privacidad de las gafas inteligentes. Por ejemplo, la venta de cualquier aplicación que utilice reconocimiento facial o que grabe video sin encender una luz de indicación en las gafas inteligentes está restringida o prohibida en los mercados oficiales o tiendas de aplicaciones.

Aunque ya existen esfuerzos para reducir el riesgo de privacidad mencionado anteriormente por las gafas inteligentes, los métodos conocidos no son suficientes para garantizar la privacidad. Por ejemplo, el bloqueo de aplicaciones de reconocimiento facial en un mercado oficial de aplicaciones no puede restringir a los desarrolladores a desarrollar aplicaciones de reconocimiento facial.

Además, dado que la preocupación por la privacidad está relacionada con las personas alrededor de un usuario de gafas, no se puede confiar en los propietarios de las gafas. Por ejemplo, la figura 1 muestra un escenario normal que ocurre cuando una persona con unas gafas inteligentes se mueve en público. La pluralidad de personas cree que son casi anónimas en el público. En esta situación, sin embargo, una vez que un usuario de gafas toma fotos o videos de las personas a su alrededor, puede realizar un reconocimiento facial e identificar a las personas a su alrededor.

Se conocen sistemas de privacidad para sistemas de videovigilancia y sistemas para compartir videos, en donde la privacidad es preservada alterando los videos añadiendo ruido (o desenfoque) o eliminando o sustituyendo objetos privados de los videos. Por lo tanto, un inconveniente importante de tales sistemas es el hecho de que la información importante en imágenes o videos es destruida, lo que no es deseable en unas gafas inteligentes.

El documento US 2012/0177248 describe un ordenador que altera al menos la métrica o el texto en una imagen fotográfica codificada digitalmente operando un algoritmo de alteración en respuesta a los datos de entrada de usuario mientras que preserva una calidad estética general de la imagen y oculta una identidad de al menos un individuo o una ubicación geográfica que aparece en la imagen.

El artículo "A Scanner Darkly: Protecting user privacy from perceptual applications” (“Un Escáner Oscuro: Proteger la privacidad del usuario de las aplicaciones perceptivas") por Jana, A. Narayanan, y V. Shmatikov, publicado en 2013, propone una capa de privacidad para los sistemas visuales.

Por consiguiente, existe la necesidad de una estructura de privacidad que garantice la privacidad de las personas alrededor de las gafas inteligentes o los relojes inteligentes. Además, se prefiere que los propietarios de las gafas puedan seguir tomando fotos o videos de sus amigos sin violar la privacidad.

Compendio de la Invención

La invención está definida por las características de las reivindicaciones independientes. Las reivindicaciones dependientes se refieren a realizaciones preferidas.

De acuerdo con un aspecto de la presente invención, se ha propuesto una estructura de privacidad automatizada en el dispositivo para un dispositivo inteligente, tal como gafas inteligentes o relojes inteligentes. La presente invención, sin embargo, no está limitada a estos tipos particulares de dispositivos inteligentes. Por ejemplo, la presente invención también puede ser implementada en teléfonos inteligentes, teléfonos móviles, cámaras web, cámaras de acción, etc. Un objetivo de la presente invención es proteger la privacidad de las personas mientras se preserva la información suficiente. La presente invención se centra preferiblemente en la característica de la cámara del dispositivo.

La estructura de la presente invención comprende preferiblemente la característica de una detección humana en imágenes de una cámara en el dispositivo. Además, basándose en el resultado de la detección, se utiliza preferiblemente un algoritmo de rastreo robusto, ya que cualquier error en el rastreo típicamente aumentará las posibilidades de reconocimiento. Además, después de la detección y el rastreo, la estructura comprende además una anonimización inteligente.

Preferiblemente, la estructura de la presente invención proporcionará equilibrio entre privacidad y utilidad. La estructura de la presente invención es preferiblemente inteligente para preservar la privacidad mientras se mantiene la funcionalidad de la cámara y suficiente información en la imagen o video.

Debería apreciarse que, para facilitar la explicación, las realizaciones son explicadas preferiblemente para imágenes, pero la presente invención también es capaz de trabajar con videos en los que cada fotograma de video puede ser tratado como una imagen separada. Las aplicaciones actuales de procesamiento de imágenes tratan los videos de la misma manera. Debería apreciarse además que, para facilitar la explicación, la mayoría de las realizaciones son explicadas preferiblemente para gafas inteligentes, pero la presente invención también es capaz de trabajar con relojes inteligentes u otros dispositivos inteligentes, particularmente dispositivos inteligentes como se ha ejemplificado anteriormente.

Preferiblemente, la anonimización es una característica importante de la presente estructura. La anonimización preferiblemente mantiene el equilibrio entre utilidad y privacidad. La utilidad es una función de la cantidad de características o información en la imagen.

Preferiblemente, la anonimización de la cara factorizará las partes de la cara en factores de identidad y de no identidad utilizando un modelo generativo de múltiples factores. La anonimización es aplicada sobre datos factorizados combinados luego las imágenes anonimizadas son reconstruidas a partir de estos datos.

Además, la estructura residirá preferiblemente dentro del dispositivo inteligente y preferiblemente será automatizada para garantizar el cortafuegos contra cualquier tipo de intento de violación de la privacidad. La mayoría de las gafas inteligentes avanzadas han adelgazado los sistemas operativos adecuados, habitualmente, estos son apilamientos de software que se ejecutan en núcleos maduros.

El programa o estructura de la presente invención está ubicado preferiblemente en una capa de abstracción cerca del núcleo del sistema operativo, en donde dicha capa cerca del núcleo del sistema operativo no es manipulable/accesible por aplicaciones programadas por desarrolladores de aplicaciones.

La ubicación exacta de la estructura de la presente invención podría variar ligeramente dependiendo de la arquitectura del sistema operativo. Por ejemplo, las Gafas de Google tienen el sistema operativo Android ejecutándose en su núcleo. Con el fin de mantener la estructura de la presente invención a salvo de los intentos de jaqueo (piratería) de los desarrolladores, preferiblemente debería existir en la capa de bibliotecas de apilamientos de software de Android.

Debe observarse que la presente invención está compuesta preferiblemente de módulos altamente independientes. Aquí los módulos y su secuencia son definidos para la referencia, aunque la estructura también es capaz de trabajar con diferentes módulos establecidos y secuenciados.

De acuerdo con un primer aspecto, la presente invención se refiere a un método para preservar la privacidad de las personas detectadas por una cámara de unas gafas inteligentes o reloj inteligente, comprendiendo el método al menos uno de las siguientes operaciones: tomar al menos una imagen de una cara por medio de la cámara de las gafas inteligentes/reloj inteligente, detectar una cara en la imagen tomada por la cámara, generar una señal de estado si se detecta una cara en la imagen, rastrear las características de identidad de la cara detectada en caso de que se genere una señal de estado; y anonimizar las características de identidad en la imagen tomada.

Con el fin de proteger la estructura contra la manipulación, se prefiere que el método sea implementado como una estructura o programa que está ubicado en una capa cerca de la capa del sistema operativo o del núcleo, en donde dicha capa cerca de la capa del sistema operativo preferiblemente no es manipulable/accesible por aplicaciones programadas por desarrolladores de aplicaciones.

En otras palabras, en la Figura 3a se proporcionan estructuras para desarrolladores en la Estructura (iii) de Aplicación. En la Figura 3b, se proporcionan tales estructuras para desarrolladores en la capa “cocoa touch” (iii). Por lo tanto, es preferible que la estructura de la presente invención resida debajo de la capa que contiene las estructuras de aplicación para desarrolladores, p. ej., debajo de la Estructura (iii) de Aplicación en la Figura 3a y debajo de la capa “cocoa touch” (iii) en la Figura 3b. En otras palabras, se prefiere que la estructura de la presente invención resida preferiblemente debajo de la capa (iii) y encima de la capa (i). Por ejemplo, la estructura de la presente invención debería residir preferiblemente en la capa (ii) en la Figura 3a y preferiblemente en el Servicio de Medios (ii’) en la Figura 3b.

La utilización de la capa de abstracción es bien conocida en los modelos de software, p. ej., el modelo OSI de 7 capas para protocolos de red informática, la biblioteca de dibujo de gráficos OpenGL, y el modelo de entrada/salida (I/O) de flujo de bytes originado por Unix y adoptado por MS-DOS, Linux, y la mayoría de los otros sistemas operativos modernos.

Por ejemplo, la Figura 3 muestra un ejemplo de componentes de software individuales en diferentes capas de abstracción de un dispositivo operado por Android. En particular, Android es un sistema operativo basado en el núcleo de Linux con una interfaz de usuario basada en la manipulación directa, diseñada principalmente para dispositivos móviles con pantalla táctil, tales como teléfonos inteligentes y tabletas, que utilizan entradas táctiles, que se corresponden libremente con acciones del mundo real, como deslizar, tocar, pellizcar, y pellizcar hacia atrás para manipular objetos en pantalla, y un teclado virtual. A pesar de estar diseñado principalmente para entrada de pantalla táctil, también se ha utilizado en televisores, consolas de juegos, cámaras digitales, y otros dispositivos electrónicos.

Con el fin de proteger la estructura de la presente invención contra la manipulación por parte de los desarrolladores de aplicaciones, se prefiere que la estructura sea implementada como un servicio que está ubicado preferiblemente en una capa cerca de la capa del sistema operativo o del núcleo. Preferiblemente, esta capa no puede eliminar el jaqueo/manipulación por parte de los desarrolladores de aplicaciones.

El propósito de este requisito preferido es proteger la estructura de ataques de jaqueo por parte de los desarrolladores. Por lo tanto, una ubicación o implementación preferida para la estructura es preferiblemente (directamente) después de las capas que no son accesibles para los desarrolladores y/o en una capa que no es accesible por un desarrollador. Habitualmente, los desarrolladores pueden escribir un código para acceder a los servicios (cámara, altavoz, registro de llamadas) para sus aplicaciones.

En particular, casi todos los sistemas operativos avanzados de gafas o dispositivos inteligentes pueden estar divididos en capas de abstracción. Estas capas típicamente separan diferentes unidades funcionales del sistema operativo. Aunque un detalle de grano fino de estas capas de abstracción puede diferir entre sistemas operativos, en un nivel superior, estos sistemas operativos están divididos de manera preferible típicamente en:

iv) Aplicaciones o capa de aplicación;
iii) Estructuras de desarrollo, también llamadas estructura de aplicación o capa de estructura de aplicación;
ii) Servicio y Bibliotecas; y
i) Núcleo OS/Núcleo.

La estructura de la presente invención debería estar ubicada preferiblemente debajo de iii) pero encima de i). Un ejemplo de un sistema operativo Android, que es utilizado, por ejemplo, en gafas de google, se ha mostrado en la Figura 3a.

Android se basa en el núcleo basado en Linux que actúa como una capa de abstracción entre el hardware y el resto del apilamiento de software. La figura 3a muestra el núcleo basado en Linux (Núcleo del Sistema Operativo) en 505 o la capa (i). Esta capa (i) contiene elementos del núcleo o el núcleo del sistema operativo.

El nivel de software intermedio incluye Máquina Virtual y Bibliotecas. La figura 3a muestra la Máquina Virtual en 503 y las bibliotecas en 504. Este "nivel de software intermedio" es la capa (ii) en la Figura 3a. Por ejemplo, la Máquina Virtual incluye Bibliotecas Principales, que permiten que cada aplicación se ejecute en su propio proceso. Las bibliotecas son utilizadas por diferentes componentes del sistema Android, tales como las Bibliotecas de Medios, las bibliotecas 3D, etc. Por ejemplo, las bibliotecas 504 incluyen servicios y bibliotecas como OpenGL ES (estructura de gráficos) y SQLite (biblioteca de base de datos). Esta capa (ii) contiene servicios y bibliotecas del sistema operativo.

El siguiente nivel superior es la Estructura de Aplicación y las Aplicaciones. La figura 3a muestra la Estructura de Aplicación en 502 o capa (iii). La Estructura de Aplicación ofrece a los desarrolladores la capacidad de crear aplicaciones ricas e innovadoras. Los desarrolladores son libres de aprovechar el hardware del dispositivo, acceder a la información de ubicación, ejecutar servicios en segundo plano, configurar alarmas, añadir notificaciones a la barra de estado, y mucho, mucho más. Esta capa (iii) contiene estructuras de desarrollo del sistema operativo. Finalmente, en (iv) las Aplicaciones están ubicadas en 501.

Además, como otro ejemplo, se hace referencia a la figura 3b, que muestra la arquitectura de iOS, es decir, el sistema operativo que es utilizado actualmente en los dispositivos inteligentes de Apple.

La capa “Cocoa Touch” (iii) proporciona la infraestructura fundamental utilizada por la aplicación. Por ejemplo, la estructura de Fundamentación proporciona soporte de desarrollo para recopilaciones, gestión de archivos, operaciones de red, y más. Esta capa contiene estructuras de desarrollo del sistema operativo. Aunque algunos nombres en el Sistema Operativo Android e iOS son diferentes, se puede ver que las capas de abstracción del sistema operativo comprenden una capa de aplicación iv), p. ej., las aplicaciones 501 en la Figura 3a y la Aplicación (iv) en la figura 3b.

Al igual que la Estructura de Aplicación (iii) en Android, iOS también proporciona una capa similar, más concretamente, la “Cocoa Touch”, que es una estructura de UI (interfaz de usuario) para crear programas de software que se ejecuten en el sistema operativo iOS (para iPhone, iPod Touch y iPad) de Apple Inc. “Cocoa Touch” proporciona una capa (iii) de abstracción de iOS. La capa “Cocoa Touch” proporciona la infraestructura fundamental utilizada por una aplicación. Por ejemplo, la estructura de Fundamentación proporciona soporte de desarrollo para recopilaciones, gestión de archivos, operaciones de red, y más. Esta capa contiene estructuras de desarrollo del sistema operativo.

Debajo de dicha capa, está ubicada la estructura (iii) de aplicación o la capa de estructura de aplicación, por ejemplo, la estructura 502 de aplicación en la Figura 3a y (iii) Servicios de Medios (ii’) y Servicios Básicos (ii) están ubicados en la Figura 3b. En particular, los Servicios Básicos y las capas de Medios de iOS contienen bibliotecas, servicios y estructuras como SQLite, OpenGL ES, administrador de Ubicaciones, etc. Esta capa contiene servicios y bibliotecas del sistema operativo (véase la Figura 3b).

Finalmente en la capa más baja, la capa (i) se comunica directamente con el hardware (véase p. ej. la Figura 3b). Esta capa es llamada núcleo (núcleo), p. ej., el núcleo 505 del sistema operativo en la Figura 3a y el Núcleo del Sistema Operativo en la Figura 3b. Al igual que la capa del núcleo de Android, el Núcleo del Sistema Operativo actúa como una capa de abstracción entre el hardware y el resto del apilamiento de software. Esta capa contiene el núcleo o el elemento central del sistema operativo del sistema operativo.

La mayoría de los sistemas operativos de gafas inteligentes sofisticadas comprenden un núcleo del sistema operativo (p. ej., Sistema Operativo central) y una capa de abstracción de hardware (véase p. ej. "Hardware" en la Figura 3). Esta capa de abstracción de hardware gestiona los recursos de hardware y proporciona una interfaz para componentes de hardware como cámara, micrófono y altavoz, etc. Estas capas son las capas más bajas en el modelo de capa de abstracción.

Las bibliotecas y los servicios residen/existen en capas combinadas o separadas justo después de esta capa de abstracción de hardware y utilizan interfaces de abstracción de hardware para realizar sus tareas dedicadas.

Como se ha mostrado, por ejemplo, en la Figura 5 habitualmente capas hasta servicios (véanse las capas (iv) y (iii); 501 y 502) son accesibles para los desarrolladores. Por lo tanto, las capas posteriores a los servicios, por ejemplo, las capas (ii') y (ii) no se pueden eliminar la manipulación/jaqueo. De acuerdo con la presente invención, es preferible residir en la

estructura de la presente invención después de la capa de servicios, p. ej., debajo de la capa (iii) como en la capa (ii') o (ii). Además, de acuerdo con una realización adicional, se preferiría además que la estructura esté dentro de la capa del núcleo (p. ej., la capa (i)). Sin embargo, puede estar ubicada en cualquier lugar entre los servicios y la capa del núcleo.

Además, de acuerdo con una realización preferida adicional, se ha mencionado explícitamente que la estructura de acuerdo con la presente invención preferiblemente no es una "aplicación" y, por lo tanto, no requiere SDK (kit de desarrollo de software) del sistema operativo. La estructura puede ser implementada de manera preferible directamente en el núcleo utilizando lenguajes como C y C++. Además, si la estructura está ubicada justo después de los servicios, entonces también puede utilizar funciones de biblioteca como OpenGL.

Además, de acuerdo con una realización preferida adicional, la estructura de la presente invención no requiere necesariamente ser una capa de abstracción separada. Dado que está relacionado preferiblemente con una sola característica de hardware que es preferiblemente la cámara, es posible que la estructura resida dentro de las capas de abstracción actuales del sistema operativo.

Con el fin de reducir el consumo de energía, que está limitado por baterías pequeñas en gafas inteligentes o relojes inteligentes, el método funciona preferiblemente en un estado inactivo si no se detecta ninguna cara en la imagen y no se genera una señal de estado, de tal manera que no se realiza la operación de rastreo.

La operación mencionada anteriormente de rastrear características de identidad rastrea preferiblemente el movimiento de caras detectadas y/o extrae características de las caras como postura, expresión y/o forma.

La operación de anonimización es un método para eliminar preferiblemente la información de identificación facial de la imagen mientras se mantiene la mayor cantidad de información posible. Hay una pluralidad de anonimizaciones conocidas en la técnica que pueden ser implementadas en el método o estructura de acuerdo con la presente invención.

Preferiblemente, la operación de anonimización divide los datos de entrada en factores de identidad y de no identidad, en donde la anonimización es realizada preferiblemente en factores de identidad tomando un promedio de k entradas.

La presente invención también se refiere a un sistema para preservar la privacidad de las personas detectadas por una cámara de unas gafas inteligentes o un reloj inteligente, comprendiendo el sistema: un módulo de cámara para tomar al menos una imagen de una cara por medio de la cámara de las gafas inteligentes, un módulo de detección para detectar una cara en la imagen tomada por la cámara, un módulo de estado para generar una señal de estado si se detecta una cara en la imagen, un módulo de rastreo para rastrear las características de identidad de la cara detectada en caso de que se genere una señal de estado; y un módulo de anonimización para anonimizar características de identidad en la imagen tomada.

El módulo de detección, el módulo de estado, el módulo de rastreo y/o el módulo de anonimización están ubicados preferiblemente en una capa directamente por encima del núcleo del sistema operativo y por debajo de una capa de estructura de aplicación en las gafas inteligentes.

Además, la presente invención se refiere a un programa informático que comprende un código de programa ejecutable por ordenador adaptado para ser ejecutado para implementar el método de la presente invención cuando está siendo ejecutado.

En el contexto de la presente invención, el término "estructura" puede referirse a un conjunto de métodos y un sistema. Además, el término video no está restringido a imágenes de visuales en movimiento, sino que también se refiere a imágenes visuales individuales (fotos).

Breve descripción de los dibujos

La presente invención se ha descrito con más detalle a continuación en la presente memoria a modo de realizaciones ejemplares y con referencia a los dibujos adjuntos, en los que:

La Figura 1 ilustra una situación con un usuario que utiliza unas gafas inteligentes en un lugar con una pluralidad de personas;
La Figura 2 muestra los componentes básicos de unas gafas inteligentes;
La Figura 3a muestra los componentes de software básicos del Sistema Operativo Android, p. ej., tal como son utilizados en unas gafas inteligentes;
La Figura 3b muestra la arquitectura de iOS, que es utilizada actualmente en dispositivos inteligentes de Apple;
La Figura 4 muestra algunos componentes de un módulo de cámara tal como es utilizado en unas gafas inteligentes;
La Figura 5 muestra un apilamiento de software de una estructura de acuerdo con la presente invención;
La Figura 6 muestra un diagrama de flujo que ilustra las operaciones del método preferido de acuerdo con la presente invención; y
La Figura 7 muestra un diagrama de flujo adicional que ilustra las operaciones del método preferido de una realización preferida adicional de acuerdo con la presente invención.

Descripción detallada de la Invención

Algunas realizaciones preferidas de acuerdo con la presente invención se han descrito ahora con referencia a los dibujos. Con el propósito de explicación, se han expuesto diferentes detalles específicos sin apartarse del alcance de la presente invención como se ha reivindicado.

Para preservar la privacidad de los usuarios, se puede utilizar una estructura heterogénea preferida que explota la anonimización facial. En particular, tal anonimización puede ser aplicada para mejorar las cuestiones de privacidad y aumentar la confianza en la tecnología. Para aplicaciones de realidad aumentada, la estructura preferida de acuerdo con la presente invención puede hacer lo siguiente: 1) preservar la privacidad de los usuarios alrededor del dispositivo; 2) mantener las imágenes y videos de calidad de los lugares permaneciendo en estado inactivo si no se detecta a una persona en la imagen; y/o 3) mantener una utilidad decente del dispositivo anonimizando solo los factores de identidad en las imágenes.

Por ejemplo, la figura 2 ilustra los componentes de unas gafas inteligentes (también llamado "dispositivo" en la presente memoria descriptiva) de acuerdo con una realización preferida de la presente invención. El dispositivo de acuerdo con la presente invención comprende preferiblemente al menos una de las siguientes características: una memoria (no mostrada), un controlador 202 de memoria, un procesador (CPU) 203, una interfaz 204 de periféricos, circuitos RF 205, circuitos 207 de audio, un altavoz 213, un micrófono 210, un subsistema 208 de entrada y salida, un dispositivo 211 de visualización de proyección de Cristal Líquido sobre Silicio, una cámara 212, componentes 201 de software y otros dispositivos 209 de entrada o de control. Estos componentes se comunican preferiblemente sobre uno o más buses de comunicación o líneas de señal. El dispositivo puede ser cualesquiera gafas inteligentes y debería apreciarse que el dispositivo ilustrado es solo un ejemplo preferido para gafas inteligentes y el dispositivo de acuerdo con la presente invención puede tener más o menos componentes como se ha mostrado en la Figura 2. Los diferentes componentes mostrados en la Figura 2 pueden ser implementados en hardware y/o software.

La figura 3a proporciona un resumen detallado de los componentes de software preferidos de un dispositivo de la presente invención. En una realización ejemplar, los componentes de software incluyen al menos uno de los siguientes componentes: núcleo 505 del sistema operativo, bibliotecas centrales 504, una máquina virtual (bibliotecas de tiempo de ejecución) 503, una estructura 502 de aplicación y una o más aplicaciones 501. Nuevamente, el dispositivo de acuerdo con la presente invención no está restringido a los componentes mostrados, es decir, se pueden utilizar más o menos componentes de software en otras realizaciones de la presente invención.

El núcleo 505 del sistema operativo comprende preferiblemente diferentes componentes de software y controladores para controlar y gestionar tareas generales del sistema (p. ej., gestión de memoria, control del dispositivo de almacenamiento, gestión de energía, configuraciones de seguridad, etc.) y facilita la comunicación entre diferentes componentes de software y hardware. Por ejemplo, el núcleo 505 del sistema operativo puede comprender: un controlador de dispositivo de visualización, un controlador WiFi, un controlador de cámara, un gestor de energía, un controlador de memoria y/u otros controladores.

En la parte superior del núcleo 505 hay preferiblemente bibliotecas centrales 504. Estas bibliotecas comprenden preferiblemente instrucciones que le dicen al dispositivo cómo manejar diferentes tipos de datos. Estas bibliotecas centrales pueden comprender una pluralidad de módulos como el motor de navegador Web de código abierto, la base de datos SQLite, que es un repositorio útil para almacenar y compartir datos de aplicaciones, bibliotecas para reproducir y grabar audio y/o video, bibliotecas SSL responsables de la seguridad de Internet, etc.

Puede existir una máquina virtual y/o bibliotecas 503 de tiempo de ejecución en la siguiente capa. Esta capa permite preferiblemente que cada aplicación se ejecute en su propio proceso con su propia instancia de máquina virtual. Se prefiere este diseño de máquinas virtuales para garantizar que las aplicaciones individuales sean independientes de otras aplicaciones. Esta construcción con máquinas virtuales proporciona además la ventaja preferida en caso de que una aplicación falle. Con esta construcción, se puede asegurar fácilmente que las aplicaciones restantes no se vean afectadas por ninguna otra aplicación que se ejecute en el dispositivo, es decir, una aplicación bloqueada preferiblemente no influye en las otras aplicaciones en ejecución.

La siguiente capa es la estructura 502 de aplicación. Esta capa incluye los programas que gestionan las funciones básicas del dispositivo, como la asignación de recursos, el cambio entre procesos o programas y el mantenimiento del rastreo de la ubicación física del dispositivo, etc. Habitualmente, los desarrolladores de aplicaciones tienen acceso completo a la estructura 502 de aplicación. Esto permite a los desarrolladores aprovechar las capacidades de procesamiento y las características de soporte al crear una aplicación. En otras palabras, la estructura de aplicación puede verse como un conjunto de herramientas básicas que pueden ser utilizadas por un desarrollador para crear herramientas o aplicaciones más complejas.

La siguiente capa ilustrada en la Figura 3a es la capa 501 de aplicación. Esta capa comprende aplicaciones como aplicación de cámara, calculadora, galería de imágenes, etc. Típicamente, un usuario del dispositivo interactúa solo con aplicaciones (“apps”) de esta capa.

La figura 4 muestra los componentes principales de un módulo de cámara tal como se ha implementado en unas gafas inteligentes de acuerdo con la presente invención. Por ejemplo, un módulo de cámara del dispositivo de acuerdo con la presente invención incluye una lente óptica 401, tecnología 402 de sensor de imágenes, procesador 403 de señal de imagen y controlador 404. La lente 401 está configurada preferiblemente para tomar fotos de alta resolución y/o grabar videos de alta definición. El sensor 402 de imagen y/o de video convierte una imagen óptica en una señal electrónica. La mayoría de los dispositivos digitales utilizan un sensor de imagen CCD o un sensor CMOS. Ambos tipos de sensores cumplen la misma tarea de capturar la luz y convertirla en señales eléctricas. Existe una comunicación entre el sensor de imagen y el procesador de señal de imagen para interpretar mejor la escena capturada con la lente. Un procesador 403 de imagen es preferiblemente un procesador de señal digital especializado utilizado para la imagen. A menudo es un sistema en un chip con arquitectura de múltiples procesadores/de procesador de múltiples núcleos. Además, al tomar videos, se puede utilizar adicionalmente un componente adicional, a menudo llamado codificador de video. El controlador 404 proporciona preferiblemente una interfaz o puente entre los chips de hardware y las bibliotecas de software.

Volviendo a la Figura 2, el subsistema 208 de I/O proporciona una interfaz entre los periféricos de entrada y salida en el dispositivo. En una realización ejemplar de acuerdo con la presente invención, un subsistema de I/O tiene un módulo 210 de voz que comprende, por ejemplo, un micrófono y/o un controlador de voz lleno de potencia. El módulo 210 de voz proporciona una interfaz de entrada entre el usuario y el dispositivo. Por ejemplo, el módulo 210 de voz recibe señales de voz (señales acústicas) del usuario y convierte estas señales acústicas en señales eléctricas. Las señales de voz podrían ser comandos que permiten a los usuarios controlar y navegar a través de diferentes características (tales como menús, cámara, etc.) del dispositivo. Por ejemplo, un usuario de las Gafas de Google puede decir comandos como "ok gafas tomar una foto" para tomar fotos con la cámara del dispositivo.

En algunas realizaciones, el dispositivo puede contener adicionalmente un módulo 209 de movimiento para activar y desactivar diferentes funciones. Este módulo 209 comprende preferiblemente un sensor de detección de movimiento, tal como un sensor giroscópico o un sensor acelerómetro. Este módulo puede ser utilizado para traducir el movimiento del usuario en comandos utilizados para controlar el dispositivo.

Algunas realizaciones también utilizan el módulo 212 de cámara como una interfaz de entrada. Por ejemplo, la pantalla de proyección del dispositivo superpone contenido de realidad aumentada frente a un usuario, en donde la entrada es creada tocando una sección particular del contenido. Un módulo de cámara selecciona el "tacto virtual" de los usuarios y lo convierte en una señal de entrada.

La presente invención proporciona una estructura de privacidad automatizada en el dispositivo para gafas inteligentes. En otras palabras, de acuerdo con la presente invención, unas gafas inteligentes están provistas de un módulo que es presentado dentro de las gafas inteligentes para garantizar la privacidad de las personas detectadas por la cámara de las gafas inteligentes. En otras palabras, el término "en el dispositivo" debería ser interpretado como un componente que ya está integrado en el dispositivo y, preferiblemente, no es manipulable por el software instalado después (aplicaciones) en el dispositivo. Debido a esta implementación "en el dispositivo", se puede garantizar la privacidad de las personas reconocidas por la cámara del dispositivo.

La efectividad de la estructura de la presente invención depende de su ubicación dentro del dispositivo. En el sentido de la presente invención, la ubicación no es preferiblemente la ubicación física, sino la ubicación o disposición en la imagen de componentes de software o capas de software como se ha ilustrado en las Figuras 3, 5 y 6. En otras palabras, ubicación significa el nivel en el que está ubicado la estructura y las interfaces correspondientes.

Preferiblemente, la ubicación de la estructura depende de la arquitectura del sistema operativo utilizado dentro de las gafas inteligentes. Sin embargo, la mayoría de los sistemas operativos en gafas inteligentes son apilamientos de software, que tienen cierto grado de similitud en su arquitectura.

La figura 5 representa una ubicación preferida de la estructura en el caso de unas gafas inteligentes que tienen el sistema operativo Android. En particular, la figura 5 muestra el nivel de accesibilidad de los desarrolladores de aplicaciones con respecto a las capas del sistema operativo. Los desarrolladores de aplicaciones habitualmente pueden acceder a la capa de estructura de aplicación del dispositivo.

La figura 5 también muestra que la ubicación de la estructura de acuerdo con la presente invención debería estar preferiblemente cerca del núcleo del sistema operativo. De acuerdo con una realización preferida adicional, puede estar ubicado justo al lado del controlador de la cámara. Esta ubicación permitirá que la estructura funcione de manera automatizada y preferiblemente la oculta de los intentos de jaqueo de los desarrolladores. En otras palabras, se prefiere que la estructura se ejecute automáticamente en una capa que no sea manipulable por un usuario.

La estructura de la presente invención está compuesta preferiblemente por cuatro componentes principales, que se han mostrado en la figura 6. En una realización ejemplar, el usuario del dispositivo utiliza cualquier método de entrada explicado antes, para girar el módulo de cámara para tomar imágenes. La estructura recibe entrada directa del módulo 301 de cámara, en donde esta entrada puede ser imágenes y/o videos. Después de seguir algunas operaciones, la estructura transforma las entradas en salidas de privacidad preservada. Sin embargo, se puede ver que la privacidad está muy afectada por eliminar la posibilidad de reconocer a una persona en la entrada (imagen o video) a través de

cualquier tecnología actual. La estructura funciona preferiblemente en dos estados.

Primero, si no se ha detectado ninguna cara (operación 305) por un módulo 302 de detección en las imágenes, entonces el módulo 303 de estado mantendrá la estructura en un estado inactivo. En otras palabras, no se generará señal de estado. De acuerdo con otra implementación, una señal de estado está presente pero es "falsa" o 0 (cero).

En segundo lugar, si se ha detectado una cara (operación 304), el módulo 303 de estado enviará una entrada a otros componentes. En otras palabras, se generará una señal de estado. De acuerdo con una implementación adicional, se generará una señal de estado "verdadero" o un "1" que indica que se ha detectado una cara.

El rastreo 306 se aplicará entonces en la cara detectada. Preferiblemente, la salida 302 de detección se convertirá en entrada del rastreo 306. Finalmente, utilizando la salida del rastreo 306, el módulo 307 de anonimización eliminará la información de identificación de la imagen.

En un sistema automatizado – tal como el sistema de esta invención – la detección facial 302 debería cumplir preferiblemente los criterios necesarios para el éxito dada la limitada memoria computacional y de computadora. Preferiblemente, el sistema debería funcionar rápidamente y con un rendimiento suficientemente alto en términos de tasa de detección de positivo verdadero/falso. Esto es un desafío ya que un área de búsqueda típica es preferiblemente la vista completa de la cámara, que a menudo es tan grande como 800 por 550 píxeles. Los algoritmos actuales cumplen con este desafío y pueden realizar la detección en tiempo real. Por ejemplo, algunas realizaciones utilizan una estrategia de búsqueda de múltiples escalas y/o múltiples escenas, que permite buscar en todo el campo de visión a una velocidad de búsqueda considerablemente más alta.

Los algoritmos de búsqueda de múltiples escalas buscan inicialmente caras en baja resolución y cambian a alta resolución solo cuando la búsqueda indica una forma de cabeza. Los métodos de búsqueda de múltiples escenas buscan escenas faciales fáciles de detectar al principio. Por ejemplo, la presencia de la cara en el campo de visión a menudo crea discontinuidades en los dominios de color de imagen o video. Buscar múltiples escenas para estas discontinuidades y examinar más a fondo solo aquellas áreas donde existe discontinuidad. Sin embargo, otros métodos pueden ser utilizados por otras realizaciones.

En realizaciones preferidas, el módulo 303 de estado de la estructura controla el estado de funcionamiento de la estructura. El módulo 303 de estado funciona con el módulo 302 de detección. Si se detecta 304 una persona o una cara en la imagen, el módulo de estado activará otros componentes de la estructura transfiriendo la salida del módulo de cámara (imágenes o videos) a la estructura; preferiblemente una señal de estado es "verdadera". Sin embargo, si el módulo 302 de detección no detecta (operación 305) ninguna cara, el módulo 303 de estado mantendrá inactivos otros componentes de la estructura inactivos al no enviarles entradas; preferiblemente la señal de estado es "falsa". Por lo tanto, el módulo 303 de estado puede ahorrar batería y potencia computacional limitadas.

Si el resultado de la detección facial 302 es verdadero, el módulo 303 de estado envía la entrada al módulo 306 de rastreo. El rastreo 306 es preferiblemente eficiente y robusto, de tal manera que el rastreo determina preferiblemente la posición, el tamaño y la postura de la cara. En una realización preferida, este módulo crea una máscara de características de la cara detectada. Una máscara de características es un conjunto de parámetros para caracterizar la identidad, el movimiento, el estado, la expresión de la postura, etc. Por ejemplo, uno de tales algoritmos es el Modelo de Apariencia Activa (AAM), que crea inicialmente un modelo de cara aplicando series de transformación y tomando la forma media del conjunto inicial de imagen de la cara. El algoritmo utiliza entonces la comparación con este modelo para estimar las características de las caras (postura, expresión, forma, etc.) en nuevas imágenes.

Debería observarse que, independientemente del método utilizado, el módulo 306 de rastreo depende preferiblemente de los resultados del módulo 302 de detección. En algunas realizaciones, el rastreo 306 utiliza un resultado de la detección 302 como una aproximación inicial para reducir el área de escaneo de la imagen. También se debería tener en cuenta que si se detecta más de una cara 302 en la imagen, el módulo 306 de rastreo realizará un rastreo de cada cara en la imagen.

Después del rastreo 306, la presente invención incluye una anonimización 307. La anonimización significa la eliminación de la información de identificación de las imágenes o videos, antes de compartir datos. El objetivo de este módulo es proteger la identidad y preservar la utilidad, p. ej., la capacidad de reconocer el género o las expresiones faciales de las imágenes anonimizadas. Aquí la utilidad de datos es una función, que asocia cada imagen. Se supone preferiblemente que para cada imagen de la cara se conoce la clase correcta. Los ejemplos de clases de imágenes incluyen expresiones faciales {neutral, sonrisa}, género {masculino, femenino}, y estado de los ojos {abierto, cerrado}.

Existen muchos algoritmos que proporcionan rendimiento y privacidad demostrables. Por ejemplo, en los siguientes artículos se analiza la anonimización con más detalle: E. Newton, L. Sweeney, y B. Malin; “Preserving privacy by de-identifying facial images” ("Preservar la privacidad anonimizando las imágenes faciales"; Transacciones de IEEE sobre Conocimiento e Ingeniería de Datos, 2005. R. Gross, E. Airoldi, B. Malin, y L. Sweeney; “Integrating utility into face de-identification” ("Utilidad integradora en la anonimización facial"); en Taller sobre Tecnologías de Mejora de la Privacidad (PET), junio de 2005. Gross, R., Sweeney, L., de la Torre, F., Baker, S.: “Model-based face de-identification";

(“Desidentificación facial basada en modelos"); Taller sobre Investigación de Privacidad en Visión. IEEE (2006)

Como referencia, un método preferido para la realización ejemplar se ha explicado en la figura 7. Utilizando el resultado del rastreo activo del modelo de apariencia, este método divide la imagen en conjuntos de características 802 y 803 de identidad y de no identidad. Las características 803 de identidad incluyen la posición y la forma de los ojos, la nariz, y los labios, etc. Las características 803 de no identidad incluyen postura, iluminación, expresiones faciales. Las técnicas de segmentación actuales se pueden aplicar con este propósito. Otros métodos aplican la anonimización 804, tomando el promedio de conjuntos de características de identidad de k imágenes. El conjunto de características de identidad promedio de k imágenes es combinado con el conjunto de no identidad de cada imagen para reconstruir 805 imágenes anonimizadas.

La descripción anterior, con el propósito de explicación, se ha descrito con referencia a realizaciones específicas. Sin embargo, las exposiciones ilustrativas anteriores no pretenden ser exhaustivas o limitar la invención a la forma precisa descrita. Muchas modificaciones y variaciones son posibles a la vista de las enseñanzas anteriores. Las realizaciones se eligieron y describieron con el fin de explicar mejor los principios de la invención y sus aplicaciones prácticas, para permitir de este modo que otros expertos en la técnica utilicen mejor la invención y diferentes realizaciones con diferentes modificaciones que sean adecuadas para la utilización particular contemplada.

REIVINDICACIONES

1. Un método para preservar la privacidad de las personas detectadas por una cámara de un dispositivo inteligente, como unas gafas inteligentes, comprendiendo el método las operaciones de:

tomar al menos una imagen de una cara por medio de la cámara del dispositivo inteligente,
detectar una cara en la imagen tomada por la cámara,
generar una señal de estado si se detecta (304) una cara en la imagen,
rastrear características de identidad de la cara detectada en caso de que se genere una señal de estado; y
anonimizar las características de identidad en la imagen tomada eliminando la información de identificación facial de la imagen.
en donde el método es implementado como un programa o estructura que está ubicado sobre una capa directamente por encima del núcleo (i) del sistema operativo y por debajo de una capa de estructura de aplicación en el dispositivo inteligente, en donde dicha capa anterior no es manipulable/accesible por aplicaciones programadas por desarrolladores de aplicaciones.

2. El método de la reivindicación 1, en donde el método es implementado como un programa o estructura que está ubicado en

a) las bibliotecas y la capa de máquina virtual en un sistema operativo Android, o
b) en la Capa de Medios en un sistema operativo iOS.

3. El método de cualquiera de las reivindicaciones anteriores, en donde el método funciona en un estado inactivo si no se detecta (305) ninguna cara en la imagen y no se genera ninguna señal de estado, de tal manera que no se realiza la operación de rastreo.

4. Método de cualquiera de las reivindicaciones anteriores, en donde la operación de rastrear características de identidad rastrea el movimiento de caras detectadas y/o extrae características de las caras como postura, expresión y/o forma.

5. Método de cualquiera de las reivindicaciones anteriores, en donde la operación de anonimización evita el pixelado indebido y/o el desenfoque de la imagen, de tal manera que la imagen siga siendo útil para los amigos.

6. Método de cualquiera de las reivindicaciones anteriores, en donde la operación de anonimización divide los datos de entrada en factores de identidad y de no identidad.

7. Un sistema para preservar la privacidad de las personas detectadas por una cámara de un dispositivo inteligente, como unas gafas inteligentes, comprendiendo el sistema:

un módulo (301) de cámara para tomar al menos una imagen de una cara por medio de la cámara del dispositivo inteligente,
un módulo (302) de detección para detectar una cara en la imagen tomada por la cámara,
un módulo (303) de estado para generar una señal de estado si se detecta una cara (304) en la imagen,
un módulo (306) de rastreo para rastrear características de identidad de la cara detectada en caso de que se genere una señal de estado; y
un módulo (307) de anonimización para anonimizar características de identidad en la imagen tomada eliminando la información de identificación facial de la imagen,
en donde el módulo (302) de detección, el módulo (303) de estado, el módulo (306) de rastreo y el módulo (307) de anonimización están ubicados sobre una capa directamente por encima del núcleo del sistema operativo y por debajo de una capa de estructura de aplicación en el dispositivo inteligente, en donde dicha capa anterior no es manipulable/accesible por aplicaciones programadas por desarrolladores de aplicaciones.

8. El sistema de la reivindicación 7, en donde el método es implementado como un programa o estructura que está ubicado en

a) las bibliotecas y la capa de máquina virtual en un sistema operativo Android, o
b) en la Capa de Medios en un sistema operativo iOS.

9. Programa informático que comprende un código de programa ejecutable por ordenador adaptado para ser ejecutado para implementar el método de cualquiera de las reivindicaciones 1-6 del método anterior cuando está siendo ejecutado.

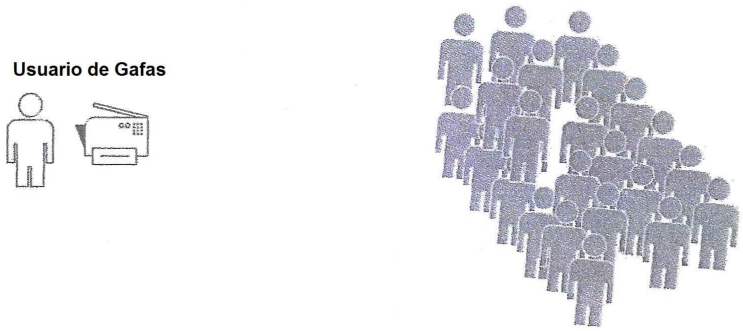
Usuario de Gafas

Fig. 1

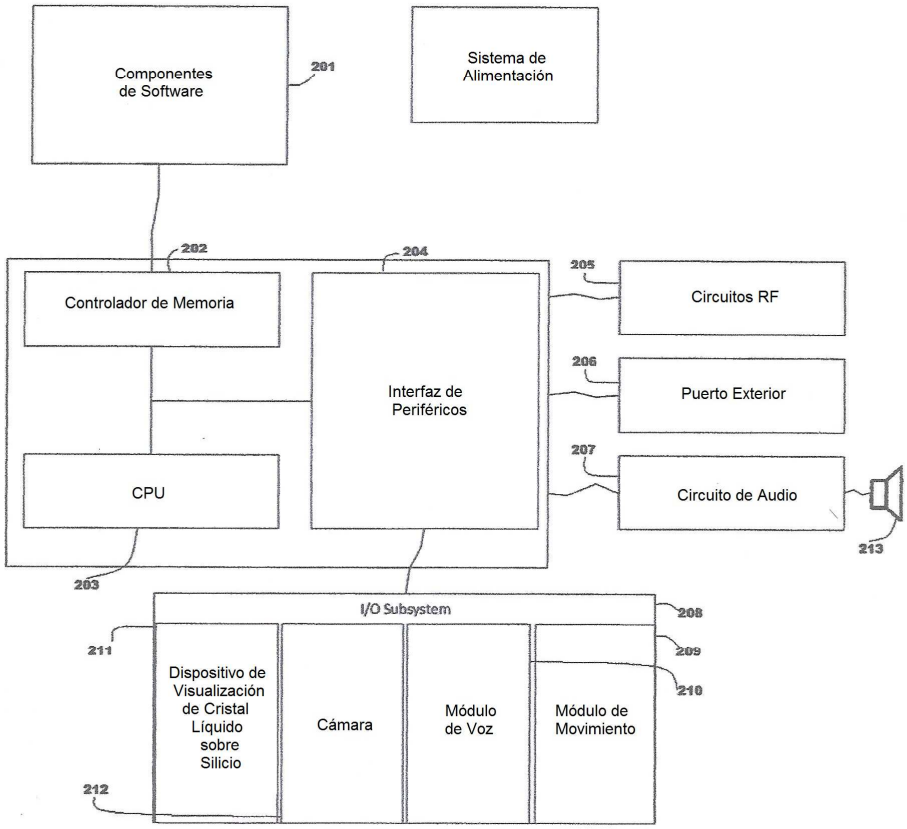
Componentes de Software
201
Sistema de Alimentación
202
204
205
Controlador de Memoria
Circuitos RF
206
Interfaz de Periféricos
Puerto Exterior
207
CPU
Circuito de Audio
213
203
I/O Subsystem
208
211
209
210
Dispositivo de Visualización de Cristal Líquido sobre Silicio
Cámara
Módulo de Voz
Módulo de Movimiento
212

Fig. 2

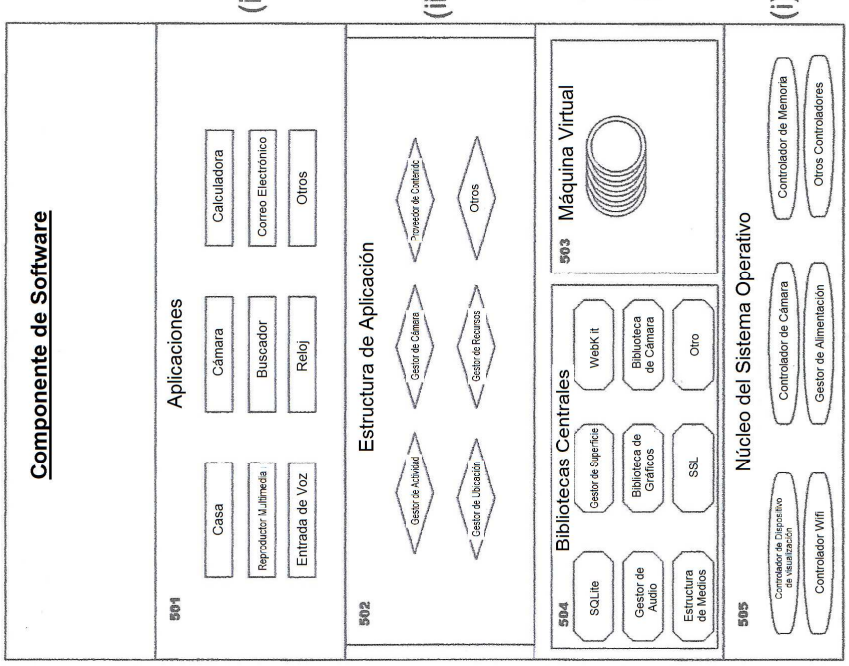
Componente de Software
501
Aplicaciones
Casa
Cámara
Calculadora
Reproductor Multimedia
Buscador
Correo Electrónico
Entrada de Voz
Reloj
Otros
(iv)
502
Estructura de Aplicación
Gestor de Actividad
Gestor de Cámara
Proveedor de Contenido
Gestor de Ubicación
Gestor de Recursos
Otros
(iii)
504
Bibliotecas Centrales
SQLite
Gestor de Superficie
WebKit
Gestor de Audio
Biblioteca de Gráficos
Biblioteca de Cámara
Estructura de Medios
SSL
Otro
503
Máquina Virtual
(ii)
505
Núcleo del Sistema Operativo
Controlador de Dispositivo de visualización
Controlador de Cámara
Controlador de Memoria
Controlador Wifi
Gestor de Alimentación
Otros Controladores
(i)

Fig. 3a

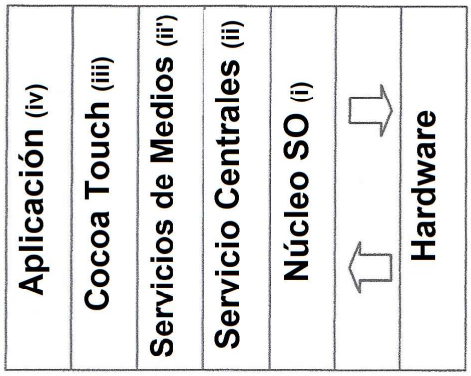
Aplicación (iv)
Cocoa Touch (iii)
Servicios de Medios (ii')
Servicio Centrales (ii)
Núcleo SO (i)
Hardware

Fig. 3b

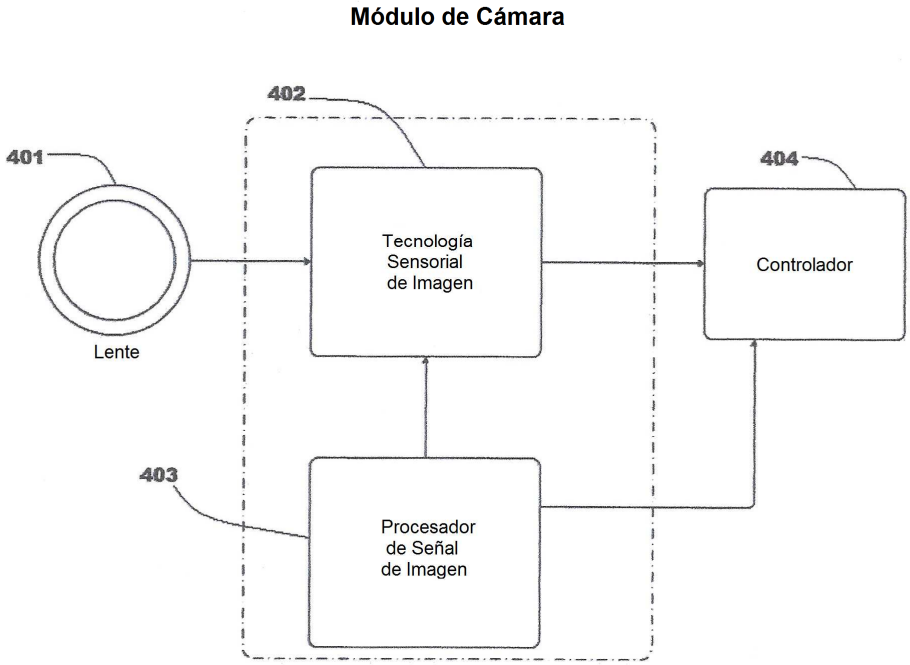
Módulo de Cámara
402
401
404
Tecnología
Sensorial
de Imagen
Controlador
Lente
403
Procesador
de Señal
de Imagen

Fig. 4

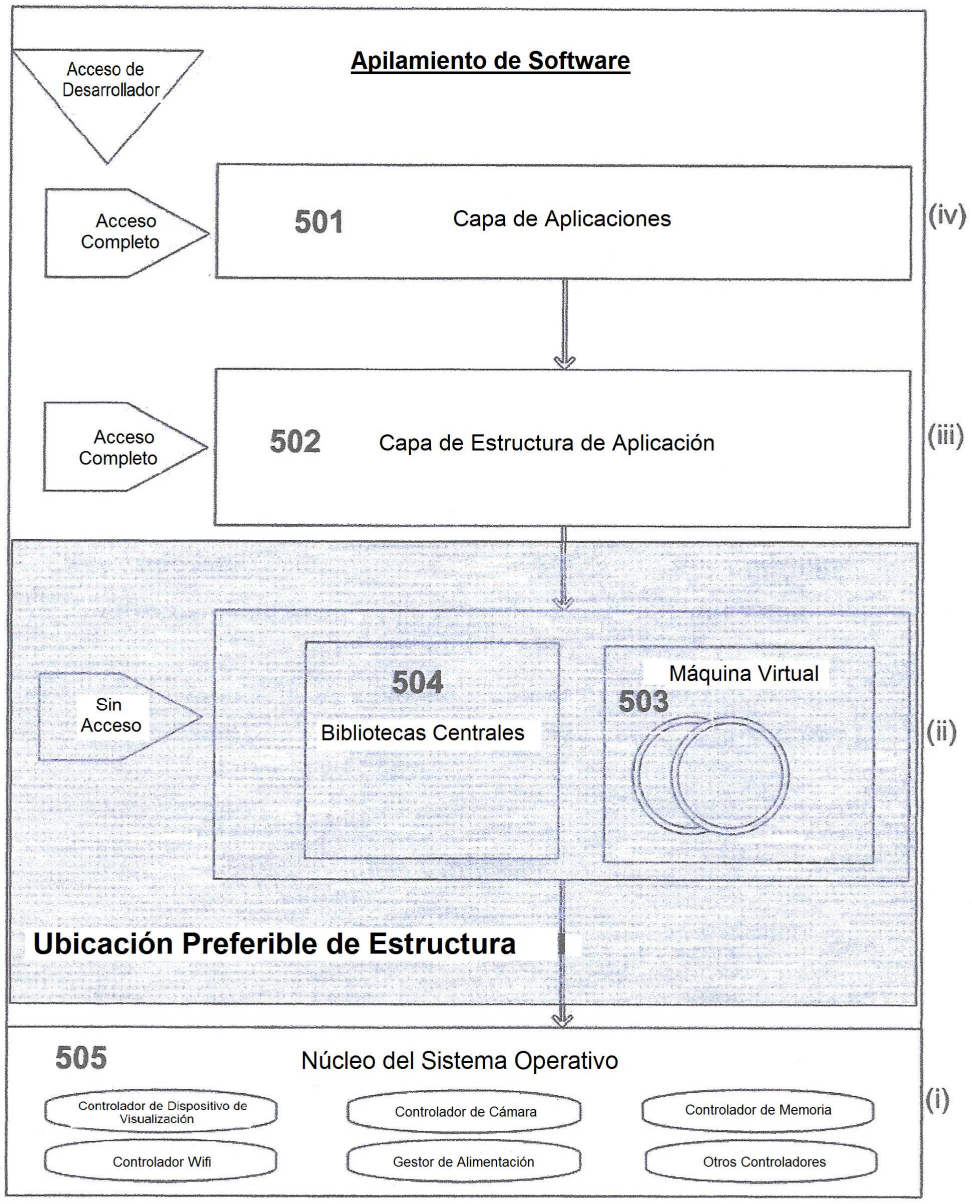
Apilamiento de Software
Acceso de Desarrollador
Acceso Completo
501
Capa de Aplicaciones
(iv)
Acceso Completo
502
Capa de Estructura de Aplicación
(iii)
Sin Acceso
504
Bibliotecas Centrales
Máquina Virtual
503
(ii)
Ubicación Preferible de Estructura
505
Núcleo del Sistema Operativo
Controlador de Dispositivo de Visualización
Controlador de Cámara
Controlador de Memoria
Controlador Wifi
Gestor de Alimentación
Otros Controladores
(i)

Fig. 5

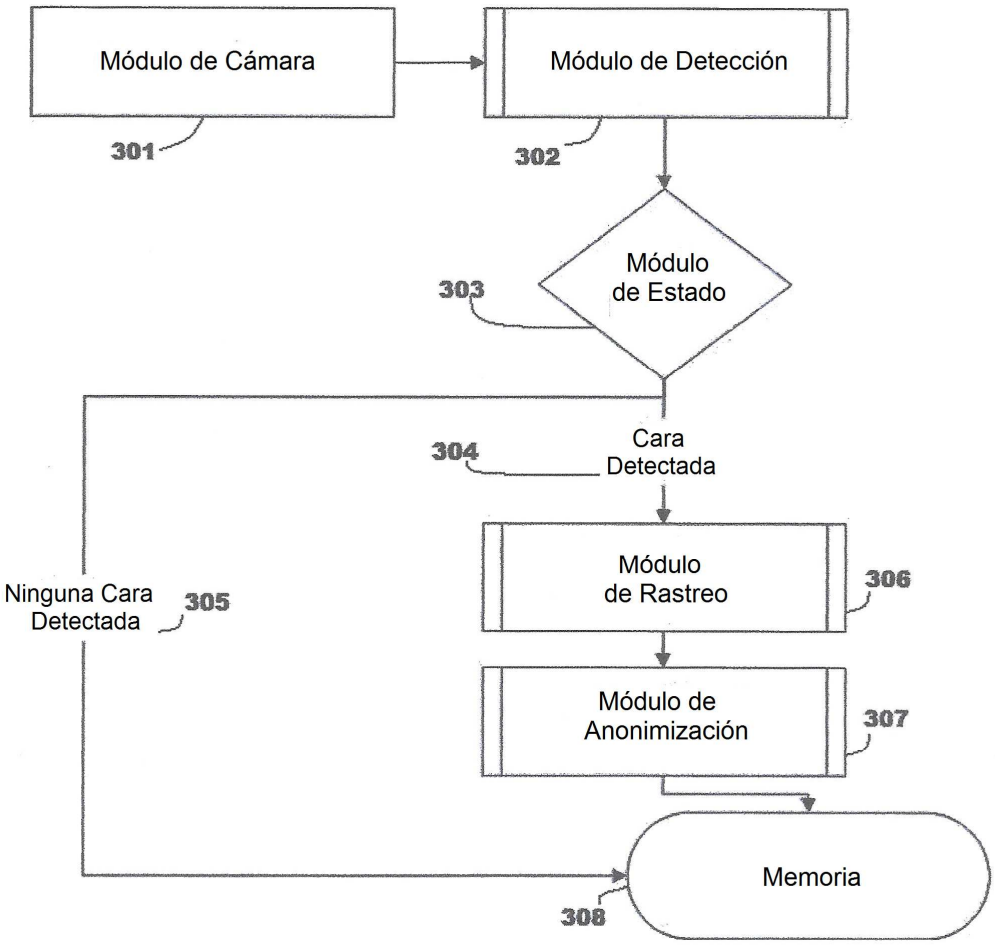
Módulo de Cámara
301
Módulo de Detección
302
Módulo
de Estado
303
Cara
Detectada
304
Ninguna Cara
Detectada
305
Módulo
de Rastreo
306
Módulo de
Anonimización
307
Memoria
308

Fig. 6

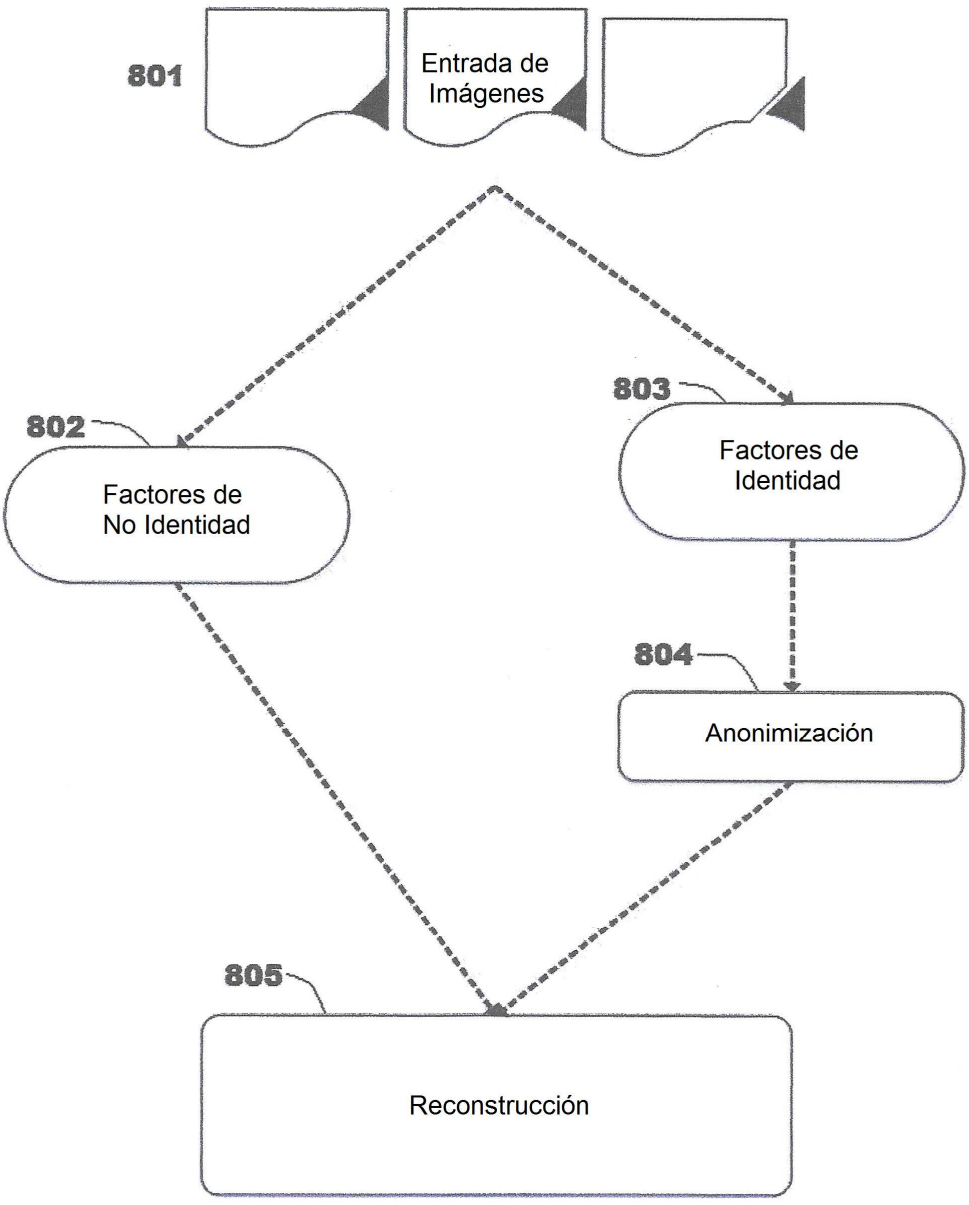
801
Entrada de Imágenes
802
Factores de No Identidad
803
Factores de Identidad
804
Anonimización
805
Reconstrucción

Fig. 7