(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 610 732**

(51) Int. CI.:

G06K 9/00 (2006.01)
G06K 9/03 (2006.01)
B42D 25/00 (2014.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.03.2014 E 14275080 (1)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2784723**

(54) Título: **Método, sistema y programa informático para comparar imágenes**

(30) Prioridad:

28.03.2013 GB 201305814
29.07.2013 US 201313953619
01.11.2013 GB 201319344

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.05.2017

(73) Titular/es:

PAYCASSO VERIFY LTD (100.0%)
20-22 Bedford Row
London WC1R 4JS, GB

(72) Inventor/es:

KING, RUSSELL

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método, sistema y programa informático para comparar imágenes

Campo técnico

La presente invención se refiere a un método, sistema y programa informático para comparar imágenes.

Antecedentes

Existe una demanda creciente para que los proveedores de servicio proporcionen sus servicios mediante dispositivos, tales como PC, tabletas y teléfonos móviles. Sin embargo, para muchos proveedores de servicio, la necesidad de verificar las credenciales de los usuarios a quienes están proporcionando un servicio es muy importante. Para los proveedores de ciertos servicios en línea, por ejemplo, existe una necesidad de asegurar que sus usuarios están por encima de una cierta edad. Como un ejemplo, los proveedores de servicio de banca en línea necesitan asegurar que la identidad de un usuario está verificada de manera fiable antes de que ese usuario se permita acceder a los servicios bancarios restringidos al usuario. Existen desafíos particulares cuando se verifica la identidad de un usuario mediante un dispositivo, en comparación con, por ejemplo, verificar una identidad de una persona mediante una transacción cara a cara.

El documento US 2006/147093A1 describe la generación de documento de identidad, y comparación de imágenes durante la autenticación. Durante la autenticación la cara de una persona que se está autenticando se fotografía y se leen datos desde un chip en el documento de identidad. Los datos de la cara fotografiada se comparan a los datos leídos desde el chip para determinar si representan el mismo usuario. En segundo lugar los datos leídos desde el chip se comparan a datos almacenados en un servidor de registro. Si los resultados desde ambas determinaciones son afirmativos, la persona se autentica.

El documento CN102456130A analiza un método y sistema para verificar el documento de identidad del usuario mediante la cara. Un método comprende: obtener información de la cara almacenada en una estructura de chip del documento de identidad, información de la cara en la instantánea impresa en el documento de identidad e información de la cara del propietario declarado del documento de identidad. La información de la cara obtenida se compara con la información de la cara almacenada en la estructura de chip y la información de la cara del propietario declarado para verificar si el propietario declarado es el poseedor legítimo del documento de identidad.

Sumario

De acuerdo con un primer aspecto de la presente invención, se proporciona un método de determinación de si un usuario de un dispositivo móvil corresponde a un usuario previamente autenticado, habiéndose autenticado previamente el usuario mediante un documento de identidad que comprende: una imagen fotográfica del usuario previamente autenticado, siendo la imagen fotográfica visible en dicho documento de identidad; y un componente de circuito integrado que almacena datos representativos de una imagen digital del usuario previamente autenticado, comprendiendo el método: provocar que un lector de chips conectado a o integral con el dispositivo móvil acceda al componente de circuito integrado, a través de lo cual recuperar dichos datos representativos de una imagen digital del usuario previamente autenticado; provocar que una cámara conectada a o integral con el dispositivo móvil capture una primera imagen, correspondiendo la primera imagen a una imagen de una porción del documento de identidad que contiene dicha imagen fotográfica visible en el documento de identidad; provocar que una cámara conectada a o integral con el dispositivo móvil capture una segunda imagen, correspondiendo la segunda imagen a un usuario del dispositivo móvil; y, disponer que dichos datos recuperados y datos indicativos de dicha primera y segunda imágenes se comparen, a través de lo cual determinar si la primera imagen, la segunda imagen y la imagen digital representan el mismo usuario; y, en el caso de que se determine que la primera imagen, la segunda imagen y la imagen digital representan el mismo usuario, formar una asociación entre el usuario previamente autenticado, y el dispositivo móvil, en el que la asociación verifica el dispositivo móvil como un dispositivo móvil del usuario previamente autenticado.

La etapa de comparar los datos recuperados y los datos indicativos de la primera y segunda imágenes, puede realizarse basándose en cada posible permutación de los datos recuperados y los datos indicativos de la primera y segunda imágenes. Como alternativa, puede emplearse un proceso menos intenso para el procesador, en el que los datos recuperados se comparan a los datos indicativos de la primera imagen, y de manera separada a los datos indicativos de la segunda imagen.

Formando una asociación entre el usuario previamente autenticado y el dispositivo móvil, el dispositivo móvil está, en efecto, verificado como el dispositivo móvil del usuario previamente autenticado. La asociación puede usarse para varios fines.

Como un primer ejemplo, la asociación puede usarse por una tercera parte que proporciona acceso a servicios o recursos restringidos para el usuario mediante dispositivos móviles. Más específicamente, la asociación puede

usarse por una tercera parte para determinar el dispositivo móvil en el que proporcionar acceso a un servicio/recurso que se ha solicitado por el usuario previamente autenticado. En este caso, tras determinar que la primera imagen, la segunda imagen y la imagen digital representan al mismo usuario, la tercera parte puede informarse del dispositivo móvil con el que está asociado el usuario previamente autenticado. De esta manera, la tercera parte puede estar segura de que los servicios o recursos que proporciona se están suministrando a un dispositivo móvil que se sujeta por el usuario previamente autenticado.

Como otro ejemplo, la asociación puede usarse para identificar comportamiento de usuario sospechoso. Por ejemplo, si un usuario de un primer dispositivo móvil está pretendiendo ser un usuario previamente autenticado; sin embargo, el usuario previamente autenticado está asociado con un dispositivo móvil diferente, y únicamente se ha autenticado a sí mismo en ese dispositivo, entonces el usuario del primer dispositivo móvil puede identificarse como un usuario sospechoso. En este caso, pueden llevarse a cabo verificaciones más estrictas en el documento de identidad suministrado por el usuario del primer dispositivo.

Como un ejemplo adicional, la asociación puede usarse para autenticar el usuario del dispositivo móvil en un evento de autenticación posterior para ese dispositivo. Más específicamente, tras determinar que la primera imagen, la segunda imagen y la imagen digital representan el mismo usuario, los datos representativos de la segunda imagen, y/o los datos representativos de la imagen digital recuperados desde el chip del documento de identidad, pueden almacenarse como una imagen validada del usuario previamente autenticado, junto con una asociación con el dispositivo móvil.

En un evento de autenticación posterior para el dispositivo móvil, la imagen almacenada del usuario previamente autenticado que está asociada con el dispositivo móvil puede recuperarse y compararse a una imagen capturada nuevamente del usuario del dispositivo móvil. De esta manera, puede determinarse si el usuario actual del dispositivo móvil es el usuario previamente autenticado asociado con el dispositivo móvil sin que se requiera que el usuario suministre un documento de identidad. En este caso, por lo tanto, la asociación entre el dispositivo móvil y el usuario previamente autenticado es, en efecto, una asociación entre el dispositivo móvil y una imagen que se ha verificado como una imagen del usuario previamente autenticado.

En la disposición específica donde la segunda imagen (es decir la imagen del usuario previamente autenticado capturada por el dispositivo móvil) se almacena como una imagen validada del usuario previamente autenticado en un dispositivo de almacenamiento remoto del dispositivo móvil, una asociación de este tipo entre el dispositivo móvil y el segundo es de uso particular. Esto es debido a que un usuario particular típicamente tendrá una pluralidad de dispositivos móviles en los que se autentica a sí mismo. Por lo tanto, el dispositivo de almacenamiento remoto puede almacenar múltiples “segundas” imágenes del usuario previamente autenticado; cada una de las cuales se capturó mediante un dispositivo móvil diferente. Almacenando una asociación entre cada una de las segundas imágenes y el dispositivo móvil que capturó la segunda imagen, la segunda imagen “correcta” puede recuperarse desde el dispositivo de almacenamiento cuando el usuario intenta autenticarse a sí mismo mediante uno de estos dispositivos. En otras palabras, cuando un usuario intenta autenticarse a sí mismo mediante un dispositivo móvil particular, la segunda imagen que se capturó mediante ese dispositivo móvil puede recuperarse desde el dispositivo de almacenamiento y compararse a una imagen capturada más nueva del usuario de ese dispositivo móvil. Comparando las imágenes que se capturaron mediante el mismo dispositivo, la fiabilidad del resultado de coincidencia de imagen puede mejorarse.

Independientemente de cómo se use la asociación, la asociación formada entre el usuario previamente autenticado, y el dispositivo móvil puede formarse, por ejemplo, almacenando una asociación entre un identificador de dispositivo único para el dispositivo móvil y datos que identifican de manera inequívoca al usuario previamente autenticado. Los datos que identifican de manera inequívoca al usuario previamente autenticado podrían comprender datos representativos de una imagen digital del usuario previamente autenticado, como se ha descrito anteriormente. El identificador de dispositivo único y los datos que identifican de manera inequívoca al usuario previamente autenticado pueden almacenarse mediante un dispositivo de almacenamiento remoto del dispositivo móvil.

Determinando si la primera imagen, la segunda imagen y la imagen digital representan el mismo usuario, puede determinarse hasta un alto nivel de confianza si el usuario del dispositivo móvil es el usuario previamente autenticado.

Más específicamente, realizando una comparación a tres bandas entre los datos recuperados y los datos indicativos de la primera y segunda imágenes, la fiabilidad del resultado de coincidencia de imagen se mejora en comparación con realizar una comparación a dos bandas entre, por ejemplo, los datos recuperados y la segunda imagen.

Adicionalmente, comparando los datos representativos de la primera imagen (es decir la imagen de la imagen fotográfica del usuario previamente autenticado visible en el documento de identidad), y los datos representativos de una imagen digital del usuario previamente autenticado almacenados en el componente de circuito integrado, la validez del documento de identidad puede verificarse. Por ejemplo, cualquier modificación realizada a la imagen fotográfica visible en el documento de identidad puede detectarse. Pueden realizarse también comprobaciones de validez adicionales.

Ventajosamente, el método puede comprender disponer que los datos recuperados y los datos indicativos de la primera imagen se comparen, para los fines de verificar la validez del documento de identidad. Por ejemplo el documento de identidad puede comprender adicionalmente primeros datos, caso en el que el método puede comprender adicionalmente disponer que los primeros datos se deriven del documento de identidad de manera que la verificación de la validez del documento de identidad se realiza basándose en los primeros datos.

En un ejemplo, al menos algunos de dichos primeros datos pueden almacenarse en el componente de circuito integrado, y la etapa de disponer que los primeros datos se deriven del documento de identidad puede comprender provocar que un lector de chips conectado a o integral con el dispositivo móvil acceda al componente de circuito integrado para recuperar dichos primeros datos. Como un ejemplo particular, los primeros datos almacenados en el componente de circuito integrado pueden comprender datos que están firmados por la autoridad que emitió el documento de identidad. En este caso, la etapa de verificar la validez del documento de identidad basándose en los primeros datos puede comprender verificar que los datos se han firmado por la autoridad emisora.

Adicionalmente o como alternativa, al menos algunos de dichos primeros datos pueden ser visibles en dicho documento de identidad, y dicha primera imagen comprende una porción del documento de identidad que contiene dichos primeros datos. En este caso la etapa de disponer que los primeros datos se deriven del documento de identidad comprende: o bien analizar rasgos en dicha primera imagen, o bien enviar dicha primera imagen a un sistema de procesamiento remoto que está configurado para analizar rasgos en dicha primera imagen, a través de lo cual derivar del documento de identidad dichos primeros datos.

Como un ejemplo particular, algunos de los primeros datos pueden almacenarse en el componente de circuito integrado y algunos pueden ser visibles en el documento de identidad. Los datos almacenados en el componente de circuito integrado pueden encriptarse con una clave que puede derivarse de los datos visibles en el documento de identidad. En este caso, la etapa de verificar la validez del documento de identidad puede comprender derivar del documento de identidad los datos visibles, y usar los datos visibles para derivar la clave para desencriptar los datos almacenados en el componente de circuito integrado. De esta manera puede verificarse, por ejemplo, que los datos visibles y/o los datos en el componente de circuito integrado no se han manipulado.

Como un ejemplo adicional, al menos algunos de los primeros datos pueden comprender un identificador único para el usuario asociado con el documento de identidad. En tales disposiciones el identificador único puede usarse para recuperar datos adicionales relacionados con el usuario desde un dispositivo de almacenamiento remoto del documento de identidad. Los datos recuperados pueden usarse para comprobar la validez del documento de identidad. Como un ejemplo específico, los datos recuperados pueden comprender una imagen del usuario asociado con el documento de identidad, y la validez del documento de identidad puede comprobarse comparando la imagen recuperada a la imagen del documento de identidad (es decir la “primera imagen”), y/o los datos representativos de la imagen digital almacenados en el chip, para verificar que el documento de identidad no se ha manipulado. Adicionalmente, o como alternativa, la imagen recuperada puede compararse a la imagen del usuario del dispositivo (es decir la “segunda imagen”). Esto puede hacerse para mejorar la fiabilidad del resultado de autenticación del usuario.

En una disposición, el documento de identidad puede comprender adicionalmente segundos datos relacionados con el usuario previamente autenticado, y el método puede comprender adicionalmente disponer que dichos segundos datos se deriven del documento de identidad. Los segundos datos pueden ser los datos que identifican al usuario previamente autenticado, tales como el nombre, fecha de nacimiento, y/o dirección del usuario. En el caso de que se determine que la primera imagen, la segunda imagen y la imagen digital representan al mismo usuario, estos segundos datos pueden almacenarse, junto con el identificador para el usuario previamente autenticado, para su uso en un evento de autenticación posterior para el usuario. Por lo tanto, el usuario no necesita proporcionar estos datos en un evento de autenticación posterior.

En un ejemplo, al menos algunos de dichos segundos datos se almacenan en el componente de circuito integrado, y dicha etapa de disponer que dichos segundos datos se deriven del documento de identidad comprende provocar que un lector de chips conectado a o integral con el dispositivo móvil acceda al componente de circuito integrado, a través de lo cual recuperar dichos segundos datos.

Adicionalmente, o como alternativa, al menos algunos de dichos segundos datos pueden ser visibles en dicho documento de identidad, y dicha primera imagen puede comprender una porción del documento de identidad que contiene dichos segundos datos. En este caso, la etapa de disponer que dichos segundos datos se deriven del documento de identidad puede comprender disponer que dichos segundos datos se extraigan de la primera imagen usando Reconocimiento Óptico de Caracteres.

Los segundos datos pueden ser un subconjunto de los primeros datos anteriormente mencionados.

En una disposición, el lector de chips puede utilizar un protocolo de Comunicación de Campo Cercano para acceder al componente de circuito integrado.

La etapa anteriormente mencionada de disponer la comparación de los datos representativos de una imagen digital del usuario previamente autenticado y los datos indicativos de la primera y segunda imágenes puede comprender, en algunas disposiciones, enviar los datos representativos de una imagen digital del usuario previamente autenticado y los datos indicativos de dicha primera y segunda imágenes a un sistema de procesamiento remoto configurado para llevar a cabo dicha comparación. Como alternativa, los datos representativos de una imagen digital del usuario previamente autenticado y los datos indicativos de dicha primera y segunda imágenes pueden compararse mediante un sistema de procesamiento del dispositivo móvil.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un sistema de procesamiento para su uso en la determinación de si un usuario de un dispositivo móvil corresponde a un usuario previamente autenticado, habiéndose autenticado previamente el usuario mediante un documento de identidad que comprende: una imagen fotográfica del usuario previamente autenticado, siendo visible la imagen fotográfica en dicho documento de identidad; y un componente de circuito integrado que almacena datos representativos de una imagen digital del usuario previamente autenticado, estando configurado el sistema de procesamiento para: provocar que un lector de chips conectado a o integral con el dispositivo móvil acceda al componente de circuito integrado, a través de lo cual recuperar dichos datos representativos de una imagen digital del usuario previamente autenticado; provocar que una cámara conectada a o integral con el dispositivo móvil capture una primera imagen, correspondiendo la primera imagen a una imagen de una porción del documento de identidad que contiene dicha imagen fotográfica visible en el documento de identidad; provocar que una cámara conectada a o integral con el dispositivo móvil capture una segunda imagen, correspondiendo la segunda imagen a un usuario del dispositivo móvil; disponer que dichos datos recuperados y datos indicativos de dicha primera y segunda imágenes se comparen, a través de lo cual determinar si la primera imagen, la segunda imagen y la imagen digital representan el mismo usuario; y, en el caso de que se determine que la primera imagen, la segunda imagen y la imagen digital representan el mismo usuario, formar una asociación entre el usuario previamente autenticado, y el dispositivo móvil, en el que la asociación verifica el dispositivo móvil (300) como un dispositivo móvil del usuario previamente autenticado.

De acuerdo con un tercer aspecto de la presente invención, se proporciona un programa informático para su uso en la determinación de si un usuario de un dispositivo móvil corresponde a un usuario previamente autenticado, habiéndose autenticado previamente el usuario mediante un documento de identidad que comprende: una imagen fotográfica del usuario previamente autenticado, siendo visible la imagen fotográfica en dicho documento de identidad; y un componente de circuito integrado que almacena datos representativos de una imagen digital del usuario previamente autenticado, y el programa informático que comprende instrucciones de manera que, cuando el programa informático se ejecuta en un sistema de procesamiento, el sistema de procesamiento está configurado para llevar a cabo un método de acuerdo con el primer aspecto.

Lo anterior proporciona un resumen de las diversas realizaciones de la presente invención. Los siguientes pasajes se refieren a características opcionales adicionales de la invención, que se describen más completamente en la descripción detallada:

En un aspecto, la presente divulgación proporciona un método de verificación, mediante un sistema de procesamiento, si un usuario de un dispositivo corresponde a un usuario previamente autenticado, teniendo acceso el sistema de procesamiento a una primera imagen y a una segunda imagen, siendo la primera imagen una imagen de un documento de identidad que comprende una imagen del usuario previamente autenticado y datos que identifican el usuario previamente autenticado, habiéndose validado el documento de identidad con respecto al usuario previamente autenticado mediante una autoridad confiable, a través de lo cual autenticar previamente al usuario, y estando dispuesto el sistema de procesamiento para derivar, del documento de identidad, dichos datos que identifican el usuario previamente autenticado, en el que la segunda imagen es una imagen capturada por el dispositivo, comprendiendo el método: comparar dicha primera imagen a dicha segunda imagen, a través de lo cual determinar si son imágenes del mismo usuario; y, en el caso de que se determine que la primera y segunda imágenes son imágenes del mismo usuario: designar una de la primera y segunda imágenes como la imagen de calidad superior; almacenar dicha imagen designada como una imagen validada del usuario previamente autenticado en un dispositivo de almacenamiento junto con un identificador para el usuario previamente autenticado, designándose dicha imagen designada para su uso en un evento de verificación posterior para el usuario previamente autenticado y; disponer que dichos datos derivados se almacenen, junto con dicho identificador para el usuario previamente autenticado, a través de lo cual posibilitar que dichos datos se recuperen en el siguiente evento de verificación para el usuario previamente autenticado.

Almacenando la imagen designada en un dispositivo de almacenamiento junto con una asociación con el usuario previamente autenticado, la imagen designada de calidad superior puede usarse como una alternativa a la imagen de calidad inferior para verificar si un usuario de un dispositivo corresponde al usuario previamente autenticado en un evento de verificación posterior.

Los documentos de identidad típicamente incluyen instantáneas del usuario con las que están asociados; sin embargo, estas instantáneas típicamente son de una calidad muy pobre para el fin de coincidencia de imagen facial. Actualmente los documentos de identidad se emiten típicamente en forma de una tarjeta u otro medio reprográfico; sin embargo, el presente método es igualmente aplicable cuando el documento de identidad tiene un componente de

identidad electrónica, por ejemplo. Un ejemplo de un componente de identidad electrónica de este tipo podría ser un chip en un documento de identidad, que almacena datos tales como una representación digital de una imagen del usuario. Como otro ejemplo, el componente de identidad electrónica podría ser un dispositivo de almacenamiento que está remoto del documento de identidad, y que almacena datos tales como una imagen digital del usuario.

Típicamente la segunda imagen, que es una imagen capturada por el dispositivo, será de una calidad superior para el fin de coincidencia de imagen facial. Por lo tanto, almacenando la segunda imagen, y usando la segunda imagen en preferencia a una imagen de un documento de identidad en un evento de verificación posterior, la fiabilidad del resultado de verificación posterior puede mejorarse.

En el caso de que se determine, en el siguiente evento de verificación, que el usuario del dispositivo es el usuario previamente autenticado, el método, en una disposición, puede comprender: usar dicho identificador para que el usuario previamente autenticado recupere los detalles derivados de la primera imagen; y, enviar dichos detalles a un sistema remoto del sistema de procesamiento junto con dicho identificador.

En una disposición, el método comprende codificar dicha segunda imagen usando un algoritmo de codificación a una banda antes de almacenar la segunda imagen codificada en dicha etapa de almacenar la segunda imagen.

El usuario previamente autenticado puede asociarse con un identificador de usuario único, y en el caso de que se determine que la primera y segunda imágenes representan al mismo usuario, el método puede comprender adicionalmente almacenar una asociación entre dicho identificador de usuario único y la segunda imagen. El identificador de usuario único puede usarse para recuperar la segunda imagen del dispositivo de almacenamiento si el usuario previamente autenticado desea posteriormente autenticarse a sí mismo en un evento de verificación posterior.

Adicionalmente, en el caso de que se determine que la primera y segunda imágenes son imágenes del mismo usuario, el método puede comprender adicionalmente enviar dicho identificador a un sistema remoto de dicho sistema de procesamiento a través de lo cual indicar que el usuario del dispositivo se ha verificado como el usuario asociado con dicho identificador. El sistema remoto del sistema de procesamiento puede ser, por ejemplo, un sistema asociado con un proveedor de servicio con el que el usuario del dispositivo desea autenticarse a sí mismo.

En el caso de que se determine que la primera y segunda imágenes son imágenes del mismo usuario, el método puede comprender adicionalmente enviar dicho identificador de dispositivo único a un sistema remoto de dicho sistema de procesamiento junto con una indicación de que el usuario del dispositivo se ha verificado. Esto puede ser particularmente útil cuando el sistema remoto del sistema de procesamiento está asociado con un proveedor de servicio como se ha analizado anteriormente, y el proveedor de servicio proporciona servicios directamente a los dispositivos.

En una disposición, dicha etapa de designar una de la primera y segunda imágenes como la imagen de calidad superior comprende la etapa de comparar la calidad de imagen de la primera imagen a la calidad de imagen de la segunda imagen. Como alternativa, puede suponerse que la segunda imagen es la imagen de calidad superior por defecto, sin realizar una comparación. Sin embargo, realizar una comparación de este tipo de las calidades de imagen de la primera y segunda imágenes asegura que la imagen de calidad superior puede usarse siempre en un evento de verificación posterior.

Ventajosamente, dicha etapa de comparar la primera imagen a la segunda imagen, a través de lo cual determinar si son imágenes del mismo usuario comprende: evaluar una calidad de imagen de cada una de una pluralidad de secciones de la primera imagen, a través de lo cual asignar una calidad de imagen a cada una de dicha pluralidad de secciones de la primera imagen; para al menos una sección de la primera imagen que se determina que tiene una calidad de imagen diferente de la calidad de imagen de otras de dicha pluralidad de secciones de la primera imagen: configurar un algoritmo de coincidencia para esa sección de la primera imagen en dependencia de la calidad de imagen asignada de esa sección de la primera imagen; y usar el algoritmo de coincidencia configurado para comparar dicha sección de la primera imagen con una sección correspondiente de la segunda imagen, a través de lo cual determinar si la primera y segunda imágenes son imágenes del mismo usuario.

La calidad de una sección de la primera imagen puede evaluarse de manera útil determinando la cantidad de detalle de la sección que contiene que es útil para realizar un proceso de coincidencia de imagen con otra imagen. Las secciones de la primera imagen que contienen pocos detalles que son útiles para coincidencia facial pueden desviar el resultado de comparación global entre la primera imagen y la segunda imagen. Considerando la calidad de imagen de la primera imagen sección a sección, las secciones de la primera imagen que contienen pocos detalles pueden identificarse, y pueden tenerse en cuenta cuando se configura el algoritmo de coincidencia, de manera que puede reducirse el efecto de desviación de estas secciones.

En una disposición, la calidad de imagen de dicha sección se determina identificando rasgos en esa sección y comparando características de dichos rasgos a características de rasgos de un conjunto de rasgos de entrenamiento predeterminado. El conjunto de imágenes de entrenamiento puede comprender uno o más conjuntos de imágenes

con rasgos “deseados” y uno o más conjuntos de imágenes con rasgos “indeseados”. Un conjunto de imágenes con rasgos deseados puede estar compuesto de imágenes que son adecuadas para comparación de imagen. Los conjuntos de imágenes que tienen rasgos indeseables pueden incluir, por ejemplo, conjuntos de imágenes con iluminación pobre o rasgos borrosos.

Como alternativa, o adicionalmente, la calidad de imagen de dicha sección puede determinarse identificando rasgos en esa sección y determinando la nitidez de los rasgos identificados. Una sección que tiene rasgos con una nitidez determinada relativamente alta puede asignarse una calidad de imagen superior que una sección que tiene rasgos con una nitidez determinada relativamente baja. La nitidez de un rasgo puede evaluarse, por ejemplo, determinando el cambio en intensidad de píxeles a través de un área dada. Un cambio grande en intensidad de píxel a través de un área relativamente pequeña podría indicar un rasgo relativamente nítido, mientras que un cambio más pequeño a través de un área más grande podría indicar un rasgo relativamente dudoso. Las secciones de una imagen que contienen rasgos nítidos típicamente contienen detalles que pueden ser útiles para coincidencia de imagen.

Opcionalmente, la primera imagen puede ser una imagen que se ha capturado mediante o en conjunto con el sistema de procesamiento. Como alternativa o adicionalmente, la segunda imagen puede ser una imagen que se ha capturado mediante o en conjunto con el sistema de procesamiento. Cuando el sistema de procesamiento es un componente de un dispositivo de usuario tal como un dispositivo móvil, la primera y/o segunda imagen pueden capturarse mediante un componente de captura de imagen del dispositivo de usuario, por ejemplo. Como alternativa, cuando el sistema de procesamiento es, por ejemplo, un servidor remoto, la primera y/o segunda imagen pueden haberse capturado mediante un dispositivo remoto del sistema de procesamiento, que está funcionando en conjunto con el sistema de procesamiento para determinar si la primera y segunda imágenes representan la misma entidad.

En el caso de que se determine que la primera y segunda imágenes no representan la misma entidad, el método puede comprender capturar de manera sucesiva imágenes adicionales mediante o en conjunto con el sistema de procesamiento, y comparar cada dicha imagen adicional con la primera imagen a través de lo cual determinar si representan la misma entidad. Esta disposición es particularmente ventajosa cuando la segunda imagen es una imagen capturada por un dispositivo móvil, puesto que las condiciones de captura de la imagen de un dispositivo móvil pueden variar (la iluminación, por ejemplo, depende enormemente de la localización y orientación del dispositivo). Por lo tanto, si se determinara erróneamente que la primera y segunda imágenes no representan la misma entidad debido a la pobre calidad de imagen de la segunda imagen, puede capturarse una imagen adicional y compararse a la primera imagen. La probabilidad de que el resultado de comparación sea correcto para la imagen adicional del usuario puede aumentarse si la imagen adicional es de calidad de imagen adecuadamente mejorada.

En una disposición, el método comprende adicionalmente comparar las calidades de imagen globales de las dos imágenes y designar la imagen con la calidad de imagen global inferior como la primera imagen y la imagen con la calidad de imagen global superior como la segunda imagen. La imagen de calidad inferior es probable que tenga un número mayor de secciones que contienen pocos detalles que son útiles para comparación de imagen, y por lo tanto la efectividad del método anterior al mejorar la fiabilidad del resultado de coincidencia de imagen puede aumentarse designando la imagen de calidad inferior como la primera imagen.

Las realizaciones pueden incluir características adicionales, tales como, un método de verificación de si el usuario de un dispositivo es un usuario que se ha autenticado previamente con respecto al usuario, en el que el dispositivo tiene acceso a una pluralidad de imágenes, al menos dos de las cuales se han capturado para el usuario en un periodo de tiempo continuo, comprendiendo el método: realizar un proceso de detección de diferencia para dichas al menos dos imágenes, comprendiendo dicho proceso de detección de diferencia: comparar dichas al menos dos imágenes a través de lo cual detectar diferencias entre ellas; y, determinar si dichas diferencias detectadas son suficientes para indicar que dichas al menos dos imágenes corresponden a un usuario vivo, a través de lo cual emitir un indicador de vitalidad; y en dependencia del indicador de vitalidad, comparar de manera selectiva una de dichas al menos dos imágenes a una imagen previamente validada de dicho usuario previamente autenticado en un proceso de coincidencia de imagen para determinar si dicha imagen comparada corresponde al usuario previamente autenticado.

Realizar un proceso de detección de diferencia de este tipo antes de comparar una imagen capturada para un usuario a una imagen previamente validada del usuario previamente autenticado asegura que la imagen capturada para el usuario es una imagen de un usuario vivo (es decir el usuario en posesión del dispositivo) y no lo es, por ejemplo, una imagen de una fotografía de un usuario no en posesión del dispositivo. Si la diferencia entre las dos imágenes se encuentra que no es suficiente, entonces el proceso de coincidencia de imagen puede no realizarse y el usuario puede no verificarse como el usuario previamente autenticado.

En el caso de que dichas diferencias detectadas se determine que no son suficientes para indicar que dichas al menos dos imágenes corresponden a un usuario vivo, el método comprende repetir dicho proceso de detección de diferencia para unas dos imágenes diferentes que se han capturado para el usuario en dicho periodo de tiempo continuo a través del cual emitir un indicador de vitalidad para dichas dos imágenes diferentes, y realizar de manera selectiva un proceso de coincidencia de imagen para una de dichas dos imágenes diferentes en dependencia del

indicador de vitalidad. Esto es útil en el caso de que el usuario del dispositivo esté permaneciendo particularmente fijo ya que permite que se detecte más tiempo de movimiento del usuario.

Adicionalmente, el método puede comprender adicionalmente repetir dicho proceso de detección de diferencia para una pluralidad de diferentes imágenes que se han capturado en dicha ventana de tiempo continua. Por lo tanto, en efecto, el usuario del dispositivo se le proporciona un tiempo predeterminado en el que puede "probar" que es un usuario vivo (es decir puede proporcionarse un tiempo predeterminado para presentar movimientos indicativos de "vitalidad"). Si el proceso de detección de diferencia no encuentra suficiente diferencia entre las imágenes capturadas en esa ventana de tiempo, puede determinarse que las imágenes no son imágenes de un usuario vivo, y por lo tanto el proceso de coincidencia de imagen puede no llevarse a cabo para el usuario.

En una disposición, dicha etapa de detectar diferencias entre dichas al menos dos imágenes comprende comparar los píxeles en una sección de una primera de dichas al menos dos imágenes a los píxeles en una sección correspondiente de las segundas de dichas dos imágenes, siendo dichas secciones secciones que se ha determinado que incluyen rasgos faciales. Pueden detectarse cambios en la expresión del usuario de esta manera y tales cambios pueden usarse para identificar una imagen de un usuario vivo.

Como alternativa o adicionalmente, dicha etapa de detectar diferencias entre dichas al menos dos imágenes puede comprender comparar los píxeles en una sección de una primera de dichas al menos dos imágenes a los píxeles en una sección correspondiente de la segunda de dichas al menos dos imágenes, siendo dichas secciones secciones que se ha determinado que incluyen tanto rasgos faciales como rasgos de fondo. Los cambios de la posición del usuario con respecto al fondo pueden detectarse de esta manera y tales cambios pueden usarse para identificar una imagen de un usuario vivo.

El sistema de procesamiento en cualquiera de los anteriores aspectos puede comprender al menos un procesador y al menos una memoria que incluye instrucciones de programa informático, la al menos una memoria y las instrucciones de programa informático están configuradas, con el al menos un procesador, para realizar los métodos anteriormente descritos. El sistema de procesamiento puede realizarse en un dispositivo de terminal de usuario tal como un dispositivo móvil, aunque ciertas funcionalidades anteriormente descritas pueden realizarse en un sistema servidor, caso en el que las imágenes pueden recibirse mediante el sistema servidor desde un dispositivo remoto del mismo. Además, las invenciones descritas en el presente documento pueden realizarse en un medio de almacenamiento legible por ordenador no transitorio que almacena dichas instrucciones de programa informático.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente una primera imagen capturada ejemplar de acuerdo con una realización de la presente invención;
La Figura 2 ilustra esquemáticamente una segunda imagen capturada ejemplar de acuerdo con una realización de la presente invención;
La Figura 3 ilustra esquemáticamente un dispositivo ejemplar configurado para llevar a cabo un método de acuerdo con una realización de la presente invención;
La Figura 4 muestra un diagrama de flujo de un método de acuerdo con una realización;
La Figura 5 ilustra esquemáticamente un primer plano de una primera imagen capturada ejemplar de acuerdo con una realización de la presente invención;
La Figura 6 ilustra esquemáticamente un dispositivo ejemplar configurado para llevar a cabo un método de acuerdo con una realización de la presente invención; y,
La Figura 7 un sistema de procesamiento ejemplar, y dispositivos ejemplares configurados para llevar a cabo un método de acuerdo con una realización de la presente invención.

Descripción detallada

Una manera convencional de verificar la identidad y/o credenciales de una persona es pedir a esa persona que proporcione documentación que apoya su identidad y/o credenciales. Por ejemplo, puede pedirse a una persona que proporcione un ID fotográfico válido, tal como un pasaporte o permiso de conducción como prueba de su identidad. En este caso, para verificar la identidad de esa persona, típicamente se realizan dos comprobaciones separadas. En primer lugar, se comprueba la validez del ID fotográfico y en segundo lugar la persona que proporciona el ID fotográfico se compara a la imagen en el ID fotográfico para verificar que el ID fotográfico pertenece a esa persona. Típicamente, estas comprobaciones se realizan por un humano.

Existen técnicas conocidas para comprobar la validez de un documento de identidad, tal como un ID fotográfico, mediante un dispositivo. Por ejemplo, configurando un dispositivo para buscar ciertos rasgos en una imagen, es posible verificar, hasta un nivel de certidumbre razonable, mediante un dispositivo, si una imagen de un documento de identidad es una imagen de un documento de identidad válido. Tales rasgos pueden incluir, por ejemplo, la inclusión de ciertos dígitos de comprobación en las zonas legibles por máquina en el documento de identidad (que pueden leerse mediante un dispositivo usando técnicas de reconocimiento óptico de caracteres (OCR)), o la inclusión de una imagen de una cara humana que está localizada en una posición esperada con relación a otros

rasgos del documento. Otros indicadores de validez incluyen, por ejemplo, la inclusión de marcas de agua u hologramas, y el uso de fuentes particulares.

Se ha reconocido por los presentes inventores que, si fuera posible realizar la segunda comprobación mediante un dispositivo, en concreto la comparación de la cara de un usuario de un dispositivo a la instantánea de una cara humana en un ID fotográfico sujeto por el usuario del dispositivo, entonces también sería posible autenticar al usuario del dispositivo de esta manera. Se ha comprobado por los presentes inventores que esto podría conseguirse configurando un dispositivo para capturar una imagen del usuario del dispositivo, y una imagen de un documento de identidad sujetado por el usuario del dispositivo, y comparar la imagen del usuario del dispositivo a la instantánea de la cara humana en el documento de identidad para determinar si representan la misma entidad. Las Figuras 1 y 2 muestran ejemplos de dos imágenes capturadas 100, 200 de este tipo.

La primera imagen 100, como se ilustra esquemáticamente en la Figura 1, es una imagen de un documento de identidad 110, que está asociada con una persona. El documento de identidad 110 contiene una instantánea 120 de la persona asociada con el documento de identidad 110. Típicamente, un documento de identidad 110 incluirá detalles 130 que pueden usarse para identificar la identidad y/u otras credenciales de la persona asociada con el documento de identidad 110. Algunos documentos de identidad 110 pueden comprender también un chip, almacenar información adicional acerca de la persona asociada con el documento de identidad 110 y pueden interrogarse mediante un lector de chips mediante un protocolo adecuado. El chip puede almacenar, por ejemplo, información biométrica, tal como una imagen digital de la persona asociada con el documento de identidad 110 y/u otra información de identificación acerca de la persona, por ejemplo nombre, dirección, etc., junto con datos relacionados con la autoridad que emitió el documento de identidad 110.

Los documentos de identidad se emiten típicamente por una autoridad confiable, tal como el gobierno, por ejemplo. Una autoridad confiable de este tipo habrá verificado anteriormente que la instantánea 120 es una instantánea de la persona asociada con el documento de identidad 110 y tendrá autenticada esa persona como la persona asociada con los detalles 130. El documento de identidad puede ser un documento físico, tal como una tarjeta de identidad, pasaporte o certificado, o puede ser un documento electrónico, tal como una fotografía digital y datos de identidad asociados.

La segunda imagen 200, como se ilustra esquemáticamente en la Figura 2, es una imagen del usuario 210 de un dispositivo, que se ha capturado por ejemplo mediante una cámara en el dispositivo. Comparando la primera y segunda imágenes 100, 200, es posible verificar si el usuario 210 del dispositivo, en el momento en el que se capturó la segunda imagen 200, es la persona asociada con el documento de identidad 110.

Existe en la técnica muchas tecnologías de reconocimiento y coincidencia facial. Para realizar de manera fiable la coincidencia requerida, la mayoría de tales tecnologías requieren que las imágenes faciales sean de una alta calidad de manera que contengan suficiente detalle distintivo para determinar si representan la misma persona. Factores que típicamente afectan la fiabilidad de coincidencia facial entre dos imágenes incluyen la resolución de las imágenes (que puede cuantificarse de manera útil como el número de píxeles entre los ojos de la persona) y la iluminación de la cara de la persona. Las imágenes con demasiada iluminación parecen como desteñidas, de manera que únicamente permanecen rasgos faciales muy intensos, tales como los ojos y la nariz, y las imágenes con demasiada poca iluminación tienen únicamente contraste muy limitado y por lo tanto los rasgos faciales intensos mencionados son menos visibles.

Las instantáneas 120 en los documentos de identidad 110 son típicamente de una baja calidad. Por ejemplo, son típicamente pequeñas, están sobre-expuestas y tienen una baja resolución. Adicionalmente, muchos documentos de identidad 110 tienen rasgos de seguridad visibles impresos sobre la instantánea 120, que pueden oscurecer detalles faciales en la instantánea 120, haciendo la coincidencia facial difícil. Si el documento de identidad 110 se convierte a imagen posteriormente, la calidad de la cara en cuestión se reduce todavía.

Las tecnologías de coincidencia facial actuales no rinden lo suficientemente bien para realizar de manera fiable una comparación entre la instantánea capturada de muy baja calidad 120 en una imagen 100 de un documento de identidad 110 y una imagen 200 de un usuario 210 de un dispositivo, que se ha capturado mediante el dispositivo. Los aspectos de la presente divulgación se refieren, por lo tanto, a proporcionar un método de coincidencia de imagen que puede comparar de manera fiable una imagen de baja calidad con otra imagen para determinar si representan la misma entidad.

La Figura 3 muestra un diagrama de bloques de un dispositivo 300 dispuesto para llevar a cabo una comparación de acuerdo con una realización ejemplar. El dispositivo 300 puede ser, por ejemplo, un teléfono móvil, un ordenador o una tableta. El dispositivo 300, en este ejemplo, comprende un sistema de procesamiento 310 y un componente de captura de imagen 320, tal como una cámara. El componente de captura de imagen 310 puede ser integral con el dispositivo 300, o puede estar separado de, pero comunicable con el dispositivo 300.

En la presente disposición, el dispositivo 300 está configurado para capturar tanto una primera imagen 100 de un documento de identidad 110 asociado con un usuario previamente autenticado, como una segunda imagen 200 de

un usuario 210 del dispositivo 300. Estas imágenes 100, 200 se proporcionan al sistema de procesamiento 310 como se ilustra esquemáticamente mediante las flechas en la Figura 3. En una disposición alternativa, el sistema de procesamiento 310 puede estar remoto del dispositivo 300, caso en el que, el dispositivo 300 puede enviar la primera y segunda imágenes 100, 200 al sistema de procesamiento 310 mediante una red alámbrica o inalámbrica, por ejemplo. Esta disposición se analiza en más detalle a continuación, con referencia a la Figura 7.

En otra disposición más, la primera imagen 100 puede haberse capturado y almacenado previamente en un dispositivo de almacenamiento, y el sistema de procesamiento 310 puede estar dispuesto para recuperar la primera imagen 100 desde el dispositivo de almacenamiento.

El sistema de procesamiento 310 está dispuesto para comparar la primera imagen 100 a la segunda imagen 200 para determinar si representan el mismo usuario (es decir para determinar si el usuario 210 representado en la segunda imagen 200 es el usuario previamente autenticado asociado con el documento de identidad 110). La Figura 4 muestra un diagrama de flujo que ilustra etapas implicadas en un proceso de comparación de este tipo.

En la etapa 400, el sistema de procesamiento 310 está configurado para evaluar una calidad de imagen de cada una de una pluralidad de secciones de la primera imagen 100, a través de lo cual asignar una calidad de imagen a cada una de la pluralidad de secciones de la primera imagen evaluadas 100. La Figura 5 muestra un primer plano de la primera imagen 100, que muestra la instantánea capturada 120 de un usuario previamente autenticado asociado con el documento de identidad 110. Se indican dos secciones ejemplares 500, 510 de la imagen mediante líneas discontinuas, cubriendo la primera 500 el área del ojo, y cubriendo la segunda 510 el área de la mejilla. En este ejemplo, cada una de estas secciones 500, 510 tiene asignada una calidad de imagen. La calidad de imagen asignada puede corresponder a la adecuación de esa sección para coincidencia facial, que puede verse afectada por un número de factores como se ha analizado anteriormente.

Típicamente, las imágenes están compuestas de una matriz de píxeles que tienen diferentes intensidades. En una disposición, la calidad de una sección, tal como la primera sección 500, puede evaluarse usando procesamiento de ondícula para identificar la variación en intensidad de píxel entre píxeles en un área dada en esa sección.

Más específicamente, considerando la primera sección 500 como un ejemplo, una cuadrícula de ondículas puede convolucionarse con los píxeles que componen la primera sección 500 a través de lo cual proporcionar repuestas indicativas del cambio en intensidad de píxel a través del área cubierta por la ondícula. Usando ondículas de diferentes tamaños, los rasgos de la imagen pueden identificarse y la “nitidez” de estos rasgos puede determinarse.

Por ejemplo, un cambio grande en intensidad de píxel a través de un área relativamente pequeña indicaría un rasgo relativamente nítido, mientras que un cambio menor a través de un área más grande indicaría un rasgo relativamente dudoso. Las secciones de la imagen que contienen rasgos nítidos típicamente contienen detalles que pueden usarse para coincidencia facial. Por ejemplo, las imágenes de los ojos, que típicamente contienen una gran cantidad de detalle en un área relativamente pequeña, normalmente contienen variaciones relativamente grandes en intensidad de píxel a través de una pequeña región. Las imágenes de las mejillas por otra parte, que típicamente contienen pocos detalles que sean útiles para coincidencia facial, normalmente contienen muy poca variación en intensidad de píxel a través de la totalidad del área. Por lo tanto las secciones de la imagen 100 que tiene rasgos más nítidos (es decir una variación mayor en intensidad de píxel por área de unidad) pueden asignarse una calidad superior que las secciones con rasgos menos nítidos. En este caso, la primera sección 500 es más probable que se asigne una calidad de imagen superior que la segunda sección 510.

Además, la nitidez de los rasgos identificados en una sección dada, y/u otras características de los rasgos identificados, pueden compararse a las características de los rasgos en un conjunto de imágenes de entrenamiento. El conjunto de imágenes de entrenamiento puede comprender uno o más conjuntos de imágenes con rasgos “deseados” y uno o más conjuntos de imágenes con rasgos “indeseados”. Estos conjuntos de imágenes pueden usarse para evaluar adicionalmente la calidad de una sección de una imagen 100. Por ejemplo, cuando se ha identificado una sección de la imagen 100 que tiene rasgos nítidos, las imágenes de prueba pueden usarse para determinar si aquellos rasgos nítidos es más probable que sean rasgos faciales o si es más probable que sean rasgos no faciales, tales como marcas de seguridad impresoras sobre la cara, por ejemplo. Un conjunto de imágenes con rasgos deseados puede estar compuesto de un conjunto de imágenes de caras humanas que son adecuadas para comparación facial. Los conjuntos de imágenes que tienen rasgos indeseables pueden incluir, por ejemplo, conjuntos de imágenes de caras humanas con rasgos tales como marcas de seguridad impuestos en los mismos. Los conjuntos de imágenes de entrenamiento pueden usarse también para entrenar el sistema de procesamiento 310 para distinguir entre la cara de una persona con piel clara, que se capturó en condiciones de baja iluminación, y la cara de una persona con piel más oscura.

A través del uso de tales imágenes de entrenamiento, el sistema de procesamiento 310 puede entrenarse por lo tanto para distinguir entre las características de rasgos faciales deseables y las características de rasgos indeseables. En otras palabras, las imágenes de entrenamiento pueden usarse para identificar las secciones de una imagen que es probable que sean de mayor utilidad cuando se realiza una comparación de imagen. En esta disposición, las secciones 500, 510 que se ha determinado que incluyen rasgos deseables pueden asignarse una

calidad de imagen alta con relación a las secciones con rasgos menos deseables, y/o secciones con rasgos más indeseables.

Como otro ejemplo, la calidad de una sección puede evaluarse como alternativa o adicionalmente determinando el número de píxeles por área de unidad en una sección dada. Se apreciará que hay otros indicadores de calidad de imagen, y estos pueden usarse como una alternativa o además de los anteriores para asignar calidades de imagen a secciones de la primera imagen 100.

Después de que el sistema de procesamiento 310 ha asignado calidades de imagen a una pluralidad de secciones de la primera imagen 100, el sistema de procesamiento 310 a continuación realiza un proceso de procesamiento de imagen para al menos una sección de la primera imagen 100 que se determina que tiene una calidad de imagen diferente de la calidad de imagen de las otras secciones evaluadas de la primera imagen 100. El proceso de procesamiento comprende las etapas 410 y 420. Considerando la primera sección 500 como un ejemplo, en la etapa 410, el sistema de procesamiento 310 configura un algoritmo de coincidencia para la primera sección 500 en dependencia de la calidad de imagen asignada de esa sección 500.

En la etapa 420, el sistema de procesamiento 310 usa el algoritmo de coincidencia configurado para comparar la primera sección 500 con una sección correspondiente de la segunda imagen 200 (es decir una sección de la segunda imagen 200 que cubre la misma parte de la cara que se cubre mediante la primera sección 500 de la primera imagen 100).

La sección de la segunda imagen 200 que corresponde a la primera sección 500 de la primera imagen 100 puede determinarse usando técnicas de reconocimiento facial convencionales tales como aquellas descritas anteriormente para identificar las características principales de una cara humana, tales como los ojos, nariz y boca, en cada una de la primera y segunda imágenes 100, 200. Estos rasgos pueden usarse como puntos de ancla para ajustar una cuadrícula de secciones a cada una de las imágenes 100, 200 de manera que cada sección en la cuadrícula cubre una porción predeterminada de la cara.

La salida del algoritmo de coincidencia para la primera sección 500 de la primera imagen 100 puede ser indicativa de la probabilidad de que la primera sección 500 represente una parte de una cara que está también presente en la sección correspondiente de la segunda imagen 200. El algoritmo de coincidencia puede configurarse para comparar la primera sección 500 a la sección correspondiente de la segunda imagen 200 comparando los rasgos (o características de los rasgos) en la primera sección 500 con los rasgos (o características de los rasgos) en la sección correspondiente de la segunda imagen 200 para determinar si hay una coincidencia.

Más específicamente, en una disposición, el sistema de procesamiento 310 puede comparar la primera sección 500 de la primera imagen 100 a la sección correspondiente de la segunda imagen 200 analizando en primer lugar la variación en intensidad de píxel como se ha analizado anteriormente. La variación en intensidad de píxel a través de la primera sección 500 puede representarse numéricamente. Este proceso puede repetirse para la sección correspondiente de la segunda imagen 200 generando de esta manera una representación numérica del cambio en intensidad de píxel a través de esta sección de la segunda imagen 200. Las dos representaciones numéricas pueden entonces compararse para determinar si las dos secciones tienen las mismas características de rasgos.

Para acelerar el proceso de comparación, y reducir las exigencias computacionales en el sistema de procesamiento 310, en una disposición, el tamaño de las representaciones numéricas de las secciones puede reducirse, usando análisis discriminante.

El proceso de procesamiento de imagen puede repetirse para múltiples secciones de la primera imagen 100, caso en el que el algoritmo de coincidencia está configurado de acuerdo con las calidades de imagen asignadas de múltiples secciones de la primera imagen 100 y se usa para comparar aquellas secciones de la primera imagen 100 a las secciones correspondientes de la segunda imagen 200 generando de esta manera múltiples salidas.

Finalmente, en la etapa 430, el sistema de procesamiento 310 está configurado para usar la una o más salidas desde el algoritmo de coincidencia para determinar si la primera imagen 100 incluye una imagen del usuario 210.

Evaluar la calidad de imagen de las secciones de la primera imagen 100 y configurar el algoritmo de coincidencia en dependencia de la calidad de imagen asignada de al menos una de estas secciones significa que las calidades de imagen de las diferentes secciones pueden tenerse en cuenta cuando se evalúa la significancia de una coincidencia cercana (o ausencia de la misma) entre una dada de estas secciones y la sección correspondiente de la segunda imagen 200.

En un ejemplo donde la primera sección 500 de la primera imagen 100 se asigna una calidad de imagen superior que la segunda sección 510, puede fijarse una significancia mayor, por ejemplo, a una coincidencia cercana (o ausencia de la misma) entre la primera sección 500 y la sección correspondiente a lo que se fijaría a una coincidencia cercana (o ausencia de la misma) entre la segunda sección 510 y la sección correspondiente de la segunda imagen 200.

Esto es particularmente útil cuando la primera imagen 100 generalmente es de calidad baja (como es típicamente el caso con imágenes capturadas de instantáneas 120 en documentos de identidad 110, como se ha analizado anteriormente). Esto es debido a que, si la primera imagen 100 se comparara a la segunda imagen 200 como una totalidad, una correspondencia fuerte (o ausencia de la misma) entre partes de la primera imagen 100 que tienen poco detalle (tal como las mejillas por ejemplo), puede desviar el resultado de comparación global, conduciendo a una determinación incorrecta en cuanto a si las imágenes 100, 200 representan el mismo usuario 210. En otras palabras, considerando la calidad de la primera imagen 100 sección a sección, puede configurarse un algoritmo de coincidencia que tiene en cuenta el efecto de desviación de secciones de una imagen que tienen una baja calidad de imagen.

En una disposición particular, el algoritmo de coincidencia puede configurarse para tener en cuenta estos efectos de desviación ponderando las salidas para las secciones de la primera imagen 100 y a continuación combinar las salidas ponderadas para generar un valor indicativo de la probabilidad de que la primera y segunda imágenes 100, 200 representen el mismo usuario 210. Las ponderaciones para las salidas para las secciones de la primera imagen 100 con una calidad de imagen superior pueden establecerse más altas que las ponderaciones para las salidas para las secciones con una calidad de imagen inferior. Las salidas ponderadas combinadas pueden a continuación compararse a un valor umbral para determinar si las imágenes representan el mismo usuario.

En una disposición, el algoritmo de coincidencia puede configurarse para las secciones de la primera imagen que se ha determinado que tienen una calidad de imagen por encima de un umbral predeterminado. En este caso, aquellas secciones con calidades de imagen asignadas por encima de ese umbral se comparan a las secciones correspondientes de la segunda imagen 200, y las secciones con calidades de imagen asignadas por debajo del umbral no se comparan a la segunda imagen 200. Esto reduce la exigencia computacional en el sistema de procesamiento 310 y evita que fuertes similitudes o diferencias entre aquellas secciones de baja calidad y las secciones correspondientes de la segunda imagen 200 desvíen el resultado de comparación global.

Si se determina que la primera y segunda imágenes 100, 200 son imágenes del mismo usuario 210, el usuario 210 del dispositivo 300 puede autenticarse como el usuario asociado con el documento de identidad 110. Antes de que se autentique el usuario 210 como el usuario asociado con el documento de identidad 110, el sistema de procesamiento 310 puede llevar a cabo etapas adicionales para verificar que la imagen 100 es una imagen de un documento de identidad válido, como se describirá en más detalle a continuación.

Aunque se ha descrito el método anterior para comparar dos imágenes para determinar si representan el mismo usuario 210 en el contexto de comparar una instantánea 120 en una primera imagen 100 de un documento de identidad 110 a una segunda imagen 200 de un usuario 210 de un dispositivo 300, se apreciará que el método es aplicable para comparar cualesquiera dos imágenes para determinar si representan la misma entidad. Como se ha analizado anteriormente, el método es particularmente útil cuando la primera imagen 100 es una imagen de baja calidad, tal como cualquier imagen que se capturó previamente en un medio reprográfico distinto a uno directamente asociado con el sistema de procesamiento 310, ya que los efectos de desviación de las secciones de baja calidad de la imagen en el resultado de comparación global pueden reducirse.

En general, por lo tanto, el método puede comprender una etapa preliminar de evaluar las calidades de imagen global de las dos imágenes a comparar y designar la imagen con la calidad de imagen global inferior como la primera imagen 100 y la imagen con la calidad de imagen global superior como la segunda imagen 200 antes de llevar a cabo el proceso de coincidencia de imagen como se ha descrito anteriormente.

Cuando se sabe que una de las dos imágenes a comparar es una imagen 100 de un documento de identidad 110, puede suponerse que la imagen del documento de identidad 110 es la imagen de calidad inferior (como se ha analizado anteriormente, las instantáneas 120 en los documentos de identidad 110 son, en general, de muy poca calidad para el fin de coincidencia facial).

Más en general, sin embargo, cuando el método anterior se usa para comparar cualesquiera dos imágenes faciales, las calidades de imagen pueden evaluarse con respecto a la adecuación de las imágenes para comparación facial. Los factores que afectan la adecuación de una imagen de una persona para comparación facial incluyen: si esa persona estaba estática cuando se capturó la imagen, si la persona estaba mirando a la cámara (u otro dispositivo de captura de imagen) cuando se capturó la imagen, si la persona tenía sus ojos abiertos, y si la persona estaba llevando elementos que oscurecieran su cara, tales como gafas. Como se ha mencionado anteriormente, otros factores incluyen la resolución de la imagen y la iluminación de la cara de la persona.

En una disposición, el conjunto anteriormente mencionado de imágenes de entrenamiento puede usarse para evaluar la calidad de las imágenes 100, 200. El uso de imágenes de entrenamiento para entrenar el sistema de procesamiento 310 para reconocer ciertos rasgos “deseables” y para distinguirlos de otros rasgos “indeseables” similares, como se ha analizado anteriormente. Para este fin, pueden usarse imágenes de entrenamiento para entrenar el sistema de procesamiento 310 para reconocer imágenes donde la iluminación es subóptima, por ejemplo. Por lo tanto, el sistema de procesamiento 310 puede determinar cuál de dos imágenes a comparar es la imagen de calidad inferior determinando cuáles de estas imágenes tiene los rasgos más “deseables”.

Como una etapa alternativa o adicional preliminar, el sistema de procesamiento 310 puede comparar la calidad de imagen de las dos imágenes a una calidad umbral y puede solicitar, por ejemplo, una imagen alternativa si la calidad de imagen de una de las imágenes está por debajo de la calidad umbral. Es particularmente útil comparar la calidad de la segunda imagen 200 a una calidad umbral, puesto que puede capturarse una mejor segunda imagen del usuario 210, por ejemplo, ordenando el usuario 210 del dispositivo 300 que encuentre mejores condiciones de iluminación.

Además o como una alternativa, en el caso de que la primera imagen 100 se determine que no es una imagen del usuario 210 representado en la segunda imagen 200, el dispositivo 300 puede configurarse para capturar una imagen adicional del usuario 210 y comparar esta imagen a la primera imagen 100 como se ha descrito anteriormente. De nuevo, pueden proporcionarse al usuario 210 direcciones en cuanto a cómo mejorar la calidad de la segunda imagen 200. Por lo tanto, si la primera imagen 100 fue realmente una imagen del usuario 210, pero se determinó que no era una imagen del usuario 210 debido a la calidad de imagen pobre de la segunda imagen 200, entonces la probabilidad de que el resultado de comparación sea correcto para la imagen adicional del usuario 210 puede aumentarse capturando una segunda imagen adicional, de calidad de imagen mejorada de manera adecuada.

Como se ha mencionado anteriormente, antes de que se autentique el usuario 210 como el usuario asociado con el documento de identidad 110, el sistema de procesamiento 310 puede llevar a cabo etapas para verificar que la imagen 100 es una imagen de un documento de identidad válido. En una realización ejemplar, el documento de identidad 110 puede comprender un chip que almacena datos relacionado con la identidad del usuario asociado con el documento de identidad 110, y estos datos pueden usarse para verificar que la imagen 100 es una imagen de un documento de identidad válido. Los datos pueden comprender, en particular, una imagen digital del usuario asociado con el documento de identidad 110 y/u otros datos para el usuario, tales como el nombre, dirección y/o fecha de nacimiento del usuario asociado con el documento de identidad 110. Típicamente, estos datos se encriptarán en el chip.

En una disposición, el dispositivo 300 puede configurarse para recuperar los datos desde el chip y pasar estos datos al sistema de procesamiento 310. El sistema de procesamiento puede a continuación usar estos datos para validar el documento de identidad 110. En efecto, por lo tanto, el sistema de procesamiento está configurado para derivar, del chip del documento de identidad, datos para su uso en la validación del documento de identidad, mediante el dispositivo 300. Cuando los datos están encriptados, los datos pueden desencriptarse mediante el sistema de procesamiento 310 antes de que se usen para validar el documento de identidad.

Como un ejemplo particular, cuando los datos almacenados en el chip del documento de identidad 110 comprenden una imagen digital del usuario asociado con el documento de identidad 110, el sistema de procesamiento 310 puede configurarse para comparar la imagen digital desde el chip a la primera imagen 100. Mediante este método, el sistema de procesamiento 310 puede determinar si la instantánea 120 en el documento de identidad 110 se ha manipulado (por ejemplo sustituido por una instantánea de un usuario diferente). Si la primera imagen 100 y la imagen derivada del chip se determina que representan el mismo usuario, entonces el sistema de procesamiento puede determinar que el documento de identidad 110 en la primera imagen 100 es válido.

Como alternativa, o adicionalmente, la imagen digital derivada del chip del documento de identidad 110 puede compararse a la segunda imagen 200 (es decir la imagen 200 del usuario 210 del dispositivo 300). Esta comparación puede realizarse en lugar de la comparación entre la primera y segunda imágenes 100, 200 anteriormente descritas, o además de la comparación entre la primera y segunda imágenes 100, 200. Cuando se realiza una comparación de este tipo además de la comparación entre la primera y segunda imágenes 100, 200, esto puede mejorar la fiabilidad del método de autenticación de usuario. En una disposición específica, el resultado de comparación para la segunda imagen 200 y la primera imagen 100 puede combinarse con el resultado de comparación para la segunda imagen 200 y la imagen derivada del chip. El resultado combinado puede usarse para determinar si el usuario 210 del dispositivo 300 es probable que sea el usuario asociado con el documento de identidad 110.

En una disposición, los datos almacenados en el chip del documento de identidad 110 pueden recuperarse usando comunicación de campo cercano (NFC). En una disposición de este tipo, el dispositivo 300 puede comprender un componente de lector de NFC que está configurado para recuperar los datos almacenados en el chip cuando está en proximidad cercana al chip. Como alternativa, el dispositivo 300 puede estar conectado de manera comunicativa a un lector de NFC separado mediante, por ejemplo, un puerto USB.

En una realización específica el documento de identidad 110 puede ser un Documento de Viaje Legible por Máquina electrónico (eMRtd), o un documento de identidad similar 110 que cumple con las normas eMRtd de ICAO (Autoridad de Aviación Civil Internacional). Tales documentos de identidad comprenden un chip, que puede usarse, entre otras cosas, para verificar la validez del documento de identidad 110. Existe un número de métodos mediante los cuales la validez de un documento de identidad 110 de este tipo puede verificarse usando el chip, como se detallará a continuación. Sin embargo, en primer lugar, se describirá en mayor detalle un eMRtd, o un documento de identidad similar 110 que cumple con las normas eMRtd de ICAO.

El chip de un eMRtd almacena primeros datos en una “Estructura de Datos Lógica”. Los primeros datos pueden incluir por ejemplo datos que corresponden a datos visibles en la superficie del documento de identidad 110. Como un ejemplo específico, los primeros datos pueden comprender datos que corresponden a datos que están codificados en formato de reconocimiento óptico de caracteres (OCR) en una zona legible por máquina (MRZ) del documento de identidad 110.

El chip también almacena un “Objeto de Seguridad de Documento”, que es para su uso en la verificación de la validez del documento de identidad. El Objeto de Seguridad de Documento comprende un troceo de los primeros datos. Puede comprender también una clave pública del documento de identidad 110, como se describirá en más detalle a continuación.

El Objeto de Seguridad de Documento está firmado por la autoridad emisora; es decir, el Objeto de Seguridad de Documento está encriptado con una clave privada de la autoridad emisora. La autoridad emisora puede ser, por ejemplo, un gobierno.

Para verificar la validez de un documento de identidad 110 de este tipo, el dispositivo 300 puede configurarse para leer los primeros datos y el Objeto de Seguridad de Documento desde el chip del documento de identidad 110. Los datos pueden leerse por ejemplo mediante un lector de chips, tal como un lector de comunicación de campo cercano, que es integral con, o conectado al dispositivo 300. Estos datos pueden enviarse a continuación al sistema de procesamiento 310. Tras la recepción, el sistema de procesamiento 310 puede configurarse para identificar la autoridad que emitió el documento de identidad 110 y obtener su clave pública.

La autoridad emisora puede identificarse a partir de datos derivados del documento de identidad 110. Por ejemplo, la autoridad emisora puede identificarse mediante datos codificados en una Zona Legible por Máquina del documento de identidad 110. En este caso, el sistema de procesamiento 310 puede configurarse para analizar la primera imagen 100 y extraer los datos que identifican la autoridad emisora usando técnicas de Reconocimiento Óptico de Caracteres, por ejemplo.

Habiendo identificado la autoridad emisora, la clave pública puede a continuación obtenerse, por ejemplo, desde un Directorio de Clave Pública mantenido por una tercera parte.

Como alternativa, la clave pública puede almacenarse en el chip, y puede haberse leído por el dispositivo 300 y enviarse al sistema de procesamiento 310, junto con los primeros datos y el Objeto de Seguridad de Documento.

Como alternativa, el sistema de procesamiento 310 puede haberse pre-configurado con la clave pública para la autoridad emisora.

Independientemente de cómo se recupere la clave pública, el sistema de procesamiento 310 puede configurarse para verificar la validez del documento de identidad 110 desencriptando en primer lugar el Objeto de Seguridad de Documento usando la clave pública de la autoridad emisora. El sistema de procesamiento 310 puede verificar por lo tanto que el Objeto de Seguridad de Documento es un Objeto de Seguridad de Documento válido.

Una vez desencriptado, el sistema de procesamiento 310 puede configurarse para comparar el Objeto de Seguridad de Documento desencriptado a un troceo de los primeros datos. Si hay una correspondencia, el sistema de procesamiento 310 puede verificar que los primeros datos no se han manipulado, y que el documento de identidad 110 es válido.

Además de lo anterior, los datos almacenados en el chip (es decir los primeros datos, el Objeto de Seguridad de Documento, y cualquier otro dato almacenado en el mismo) pueden codificarse. En una realización específica, los datos pueden haberse codificado usando una clave derivada de datos que son visibles en la superficie del documento de identidad. Tales datos visibles podrían incluir, por ejemplo, datos codificados en un formato de OCR en una MRZ del documento de identidad 110.

Por lo tanto, para leer los primeros datos y el Objeto de Seguridad de Documento desde el chip del documento de identidad 110, puede requerirse en primer lugar que el dispositivo 300 derive, de la superficie del documento de identidad, los datos visibles. Estos datos podrían derivarse directamente de la superficie del documento de identidad 110, o desde la primera imagen del documento de identidad 100, por ejemplo usando técnicas de OCR.

Si el sistema de procesamiento 310 puede decodificar satisfactoriamente los datos almacenados en el chip usando los datos visibles en la superficie del documento de identidad 110, puede determinarse que el chip del documento de identidad 110 no se ha sustituido, y/o que los datos visibles en la superficie del documento de identidad 110 no se han modificado.

El chip puede comprender adicionalmente un elemento seguro que contiene una clave privada para el documento de identidad 110. En este caso el dispositivo puede enviar un desafío al chip, que provoca que el chip responda con una respuesta que está firmada con la clave privada del documento de identidad 110.

Tras la recepción de la respuesta firmada, el sistema de procesamiento 310 puede configurarse para verificar, usando la clave pública del documento de identidad 110 que la respuesta se ha firmado mediante la clave privada del documento de identidad 110. Esto proporciona la garantía de que los datos almacenados en el chip del documento de identidad 110 no se han duplicado desde otro chip.

Como se apreciará, cuando el sistema de procesamiento 310 es un componente del dispositivo 300, la validez del documento de identidad se verificará por el propio dispositivo 300. Cuando el sistema de procesamiento 310 está remoto del dispositivo 300, la verificación se llevará a cabo de manera remota, y el dispositivo 300 está configurado para enviar los datos derivados del documento de identidad 110 que se requieren por el sistema de procesamiento 310 para verificar la validez del documento de identidad 110 para el sistema de procesamiento 310.

Como alternativa o adicionalmente a las comprobaciones de validez anteriormente descritas, que hacen uso de datos almacenados en un chip del documento de identidad 110 y/o datos visibles en la superficie del documento de identidad 110, pueden llevarse a cabo comprobaciones de validez a través del uso de datos que se almacenan en un dispositivo de almacenamiento remoto del documento de identidad 110. Como un ejemplo, dichos datos almacenados pueden comprender una imagen del usuario asociado con el documento de identidad 110, y esta imagen puede recuperarse desde el dispositivo de almacenamiento remoto, y compararse a una o ambas de la primera y segunda imágenes 100, 200 a través de lo cual verificar si el documento de identidad 110 es válido y para mejorar la fiabilidad del resultado de autenticación del usuario. Un dispositivo de almacenamiento remoto de este tipo podría ser, por ejemplo, un dispositivo de almacenamiento sujeto por un cuerpo gubernamental, que almacena imágenes validadas de ciudadanos.

En un ejemplo específico, la imagen almacenada por el dispositivo de almacenamiento remoto puede recuperarse a través del uso de datos derivados del documento de identidad 110 que identifican de manera inequívoca al usuario asociado con el documento de identidad 110. En otras palabras, la imagen puede recuperarse a través del uso de un identificador de usuario único derivado del documento de identidad. Un identificador único de este tipo podría incluir, por ejemplo, un código de identificador de usuario único, tal como un número de pasaporte o un número de seguridad social y podría derivarse de la superficie del documento de identidad 110 y/o un chip del documento de identidad 110, como se ha descrito anteriormente.

En el presente ejemplo, la imagen almacenada por el dispositivo de almacenamiento remoto puede recuperarse enviando en primer lugar el identificador de usuario único derivado al dispositivo de almacenamiento remoto a través de lo cual identificar el usuario asociado con el documento de identidad 110 al dispositivo de almacenamiento remoto. El dispositivo de almacenamiento remoto puede a continuación usar el identificador de usuario único para recuperar la imagen del usuario del documento de identidad 110 y puede enviar la imagen recuperada al dispositivo 300 y/o al sistema de procesamiento 310.

De acuerdo con otro aspecto, en una realización, el sistema de procesamiento 310 tiene acceso a un dispositivo de almacenamiento 600, como se muestra en la Figura 6. Una vez que se ha determinado que la primera imagen 100 del documento de identidad 110 y la segunda imagen 200 del usuario 210 del dispositivo 300 representan el mismo usuario, la segunda imagen 200 del usuario 210 pueden almacenarse como una imagen validada del usuario asociado con el documento de identidad 110 en el dispositivo de almacenamiento 600 como se muestra en la Figura 6.

Como se ha analizado anteriormente, típicamente, la segunda imagen 200 capturada por el dispositivo 300 será de una calidad superior a la primera imagen 100 del documento de identidad 110. En una disposición, si un usuario del dispositivo 300 desea más tarde autenticarse a sí mismo en el dispositivo 300 como el usuario previamente autenticado 210 asociado con el documento de identidad 110, el sistema de procesamiento 310 puede capturar una imagen posterior 200* del usuario del dispositivo 300 y puede comparar la imagen posterior 200* con la segunda imagen validada 200 para determinar si son imágenes del mismo usuario. Las imágenes pueden compararse de acuerdo con el método anteriormente descrito, o como alternativa, puede usarse un algoritmo de coincidencia facial convencional para comparar las imágenes.

En el caso de que se determine que las dos imágenes 200, 200* representan el mismo usuario, el sistema de procesamiento 310 puede autenticar el usuario del dispositivo 300 como el usuario previamente autenticado 210 asociado con el documento de identidad 110.

En la presente realización, por lo tanto, una vez que el usuario 210 se ha autenticado una vez usando una imagen 100 de un documento de identidad 110, el usuario 210 no necesita proporcionar ninguna imagen adicional de documentos de identidad 100 para autenticarse a sí mismo en eventos de autenticación posteriores. En su lugar, el usuario 210 puede autenticarse a sí mismo usando la imagen validada almacenada 200.

Adicionalmente, almacenando la segunda imagen 200, en preferencia a, por ejemplo, la primera imagen 100, la fiabilidad de eventos de autenticación posteriores puede mejorarse. Esto es debido a que la segunda imagen 200 típicamente será de calidad superior a la primera imagen 100 y por lo tanto los eventos de autenticación posteriores se llevan a cabo comparando dos imágenes de calidad relativamente alta 200, 200* entre sí, en lugar de comparar

una imagen de calidad muy baja (la primera imagen 100) a una imagen de calidad superior 200*. En efecto, por lo tanto, podría decirse que la segunda imagen 200 está designada como la imagen de calidad superior cuando se almacena. La segunda imagen validada 200 puede usarse para todos los eventos de autenticación posteriores para el usuario 210.

Como alternativa, en una disposición, si se determina que una imagen capturada posteriormente 200* de un usuario del dispositivo 300 representa el usuario previamente autenticado 210 representado en la segunda imagen validada 200, el sistema de procesamiento 310 puede almacenar también la imagen capturada posteriormente 200* como una imagen validada del usuario previamente autenticado 210 en el dispositivo de almacenamiento 600. Dos imágenes capturadas posteriormente ejemplares 200**, 200***, que se han validado previamente usando la segunda imagen 200 como que son imágenes del usuario asociado con el documento de identidad 110, se muestran esquemáticamente estando almacenadas en el dispositivo de almacenamiento 600 en la Figura 6.

El sistema de procesamiento 310 puede, en una disposición, comparar las calidades de la segunda imagen validada 200 y la imagen capturada posteriormente 200* y puede designar una como la imagen de calidad superior. Posteriormente, en un evento de autenticación posterior adicional, el sistema de procesamiento 310 puede seleccionar la imagen de calidad superior designada desde el dispositivo de almacenamiento 600 y usar esa imagen en el evento de autenticación posterior adicional, mejorando de esta manera adicionalmente la fiabilidad del resultado de comparación en el evento de autenticación posterior adicional. En una disposición, el sistema de procesamiento 310 puede asignar una calidad de imagen a cada imagen validada almacenada, y cada vez que el sistema de procesamiento 300 valida un usuario del dispositivo 300, puede seleccionar la imagen validada de la calidad más alta desde el dispositivo de almacenamiento 600 para autenticar el usuario.

Las imágenes validadas almacenadas 200, 200**, 200*** pueden codificarse con un algoritmo de codificación de una banda antes de que se almacenen. En otras palabras, las imágenes 200, 200**, 200*** pueden almacenarse como representaciones numéricas, de las que no pueden derivarse las imágenes originales. Cuando una imagen capturada posteriormente 200* de un usuario del dispositivo 300 se compara a una imagen codificada almacenada 200, 200**, 200*** en el dispositivo de almacenamiento 600, la imagen capturada posteriormente 200* se codifica posteriormente de manera similar antes de que se compare a la imagen codificada almacenada. Como se ha analizado anteriormente, la exigencia computacional en el sistema de procesamiento 310 es inferior cuando se realiza una comparación entre las representaciones numéricas de imágenes (por ejemplo imágenes codificadas), en lugar de entre las propias imágenes originales, y por lo tanto codificando imágenes antes de que se comparen, la comparación puede llevarse a cabo de manera más rápida.

El sistema de procesamiento 310 puede generar, en una disposición, o derivar de otra manera un identificador de usuario único 610 para el usuario 210 asociado con el documento de identidad 110, y puede almacenar este identificador 610 junto con la segunda imagen 200 y cualesquiera otras imágenes validadas almacenadas 200**, 200*** del usuario 210. El sistema de procesamiento 310 puede usar este identificador 610 para recuperar una imagen validada del usuario 210 desde el dispositivo de almacenamiento 600 en eventos de autenticación posteriores para el usuario 210.

En un ejemplo particular, el identificador de usuario único 610 para el usuario 210 puede ser un valor de troceo derivado de los detalles relacionados con el usuario 210. Los detalles pueden comprender, por ejemplo el nombre y apellidos del usuario 210, y la fecha de nacimiento del usuario 210. Estos detalles pueden haberse derivado del documento de identidad 110 mediante el sistema de procesamiento 310 (usando reconocimiento óptico, por ejemplo, u otras técnicas adecuadas).

Posteriormente, para identificar al usuario 210 en el sistema de procesamiento 310 en un evento de autenticación posterior para el usuario 210, únicamente necesita proporcionarse al sistema de procesamiento 310 con detalles relacionados con el usuario 210 que está siendo autenticado, de los que puede derivar a continuación el identificador de usuario único 610. El sistema de procesamiento 310 puede almacenar, como alternativa o adicionalmente, ciertos detalles de usuario en asociación con, pero de manera separada de, el identificador de usuario único.

El sistema de procesamiento 310 puede enviar también, en un ejemplo, el identificador de usuario único 610 para el usuario 210 a un servidor remoto del sistema de procesamiento 310 a través de lo cual indicar al servidor que el usuario 210 del dispositivo 300 se ha autenticado como un usuario asociado con el identificador de usuario único 610. Esto es útil, por ejemplo, cuando el usuario del dispositivo 300 está solicitando acceso a un servicio proporcionado por el servidor remoto mediante el dispositivo 300, y el servidor remoto necesita verificar la identidad del usuario 210 del dispositivo 300 antes de que proporcione el servicio.

En una disposición, el sistema de procesamiento 310 puede almacenar detalles relacionados con la identidad del usuario 210 asociado con el documento de identidad 110 junto con la imagen validada 200 del usuario 210 y/o el identificador de usuario 610. Estos detalles pueden haberse derivado, en un ejemplo, de la imagen 100 del documento de identidad 110. Por ejemplo, cuando el documento de identidad contiene detalles 130 impresos o presentados de otra manera en una superficie del documento de identidad 110 en forma de texto, estos detalles pueden extraerse usando reconocimiento óptico de caracteres y almacenarse.

Adicionalmente o como alternativa, los detalles pueden haberse derivado de datos almacenados en un chip del documento de identidad 110. Más específicamente, como se ha mencionado anteriormente, un documento de identidad 110 puede comprender un chip que almacena datos que identifican el usuario asociado con el documento de identidad 110 (por ejemplo el nombre, dirección y/o una imagen digital del usuario). El dispositivo 300 puede configurarse para recuperar los datos desde el chip (usando NFC, por ejemplo), y pasar estos datos al sistema de procesamiento 310 para almacenarse. En otras palabras, el sistema de procesamiento 310 puede almacenar datos que se han derivado de un chip del documento de identidad 110 mediante el dispositivo 300.

Adicionalmente o como alternativa, algunos o todos los detalles almacenados pueden haberse recuperado desde un dispositivo de almacenamiento remoto usando datos derivados del documento de identidad. Más específicamente, el sistema de procesamiento 310 puede configurarse, en una disposición, para derivar, del documento de identidad 110, datos que identifican de manera inequívoca al usuario asociado con el documento de identidad 110. En otras palabras, el sistema de procesamiento 310 puede configurarse para derivar del documento de identidad 110 un identificador de usuario único. El sistema de procesamiento 310 puede a continuación enviar el identificador de usuario único al dispositivo de almacenamiento remoto, y el dispositivo de almacenamiento remoto puede usar el identificador de usuario único para recuperar detalles relacionados con el usuario asociado con el documento de identidad 110, y para enviar los detalles recuperados al sistema de procesamiento 310.

Adicionalmente o como alternativa, los detalles almacenados pueden haberse proporcionado mediante el usuario 210 del dispositivo 300 cuando el usuario 210 estaba autenticado inicialmente con la primera imagen 100 del documento de identidad 110.

Además, o como una alternativa, a almacenar los datos derivados del documento de identidad de manera local en el sistema de procesamiento 310, el sistema de procesamiento 310 puede disponer que los detalles relacionados con la identidad del usuario 210 se almacenen en un dispositivo de almacenamiento 600 remoto del sistema de procesamiento 310, junto con la imagen validada 200 del usuario 210 y/o el identificador para el usuario 210. El dispositivo de almacenamiento remoto 600 podría ser un dispositivo de almacenamiento de un proveedor de servicio con el que el usuario está intentando autenticarse a sí mismo, por ejemplo.

En cualquier caso, en un evento de autenticación posterior, cuando un usuario del dispositivo 300 está autenticado como el usuario previamente autenticado 210 asociado con el documento de identidad 110, estos detalles pueden recuperarse desde el dispositivo de almacenamiento 600. Los detalles pueden enviarse, en un ejemplo, a un servidor remoto del sistema de procesamiento 310 a través de lo cual identificar el usuario autenticado en el servidor.

Como se ha mencionado anteriormente con referencia a la Figura 3, pueden usarse realizaciones para autenticar usuarios en una pluralidad de dispositivos. Cuando una imagen capturada 200* de un usuario de un dispositivo dado se determina que representa un usuario previamente autenticado 210 (o bien mediante comparación de la imagen capturada 200* con una imagen 100 de un documento de identidad 110 o bien mediante comparación de la imagen capturada 200* con una imagen almacenada 200, 200**, 200***, que se ha validado anteriormente mediante el sistema de procesamiento 310 como que es una imagen del usuario previamente autenticado 210), el sistema de procesamiento 310 puede almacenar un identificador de dispositivo único para ese dispositivo, junto con la imagen capturada 200*. Este identificador de dispositivo único podría usarse de varias maneras como será evidente en la siguiente descripción.

El identificador de dispositivo único puede usarse para identificar comportamiento de usuario sospechoso. Como un ejemplo, si un usuario de un dispositivo intenta autenticarse a sí mismo como un usuario previamente autenticado dado, pero el usuario previamente autenticado dado solo se ha autenticado a sí mismo en un dispositivo diferente, entonces el sistema de procesamiento 310 puede poder determinar, desde los identificadores de dispositivo únicos para los dispositivos, que la autenticación es una autenticación sospechosa.

Además, cuando un usuario de un dispositivo desea autenticarse a sí mismo a un servidor remoto del sistema de procesamiento 310 mediante el dispositivo, el identificador de usuario único puede enviarse a un servidor a través del cual identificar al servidor en el que el usuario del dispositivo se ha autenticado.

De acuerdo con un aspecto adicional, antes de que una imagen 200 del usuario 210 del dispositivo 300 que se ha capturado mediante el dispositivo 300 se compare a una imagen de un usuario previamente autenticado (es decir, o bien una imagen de un documento de identidad 110 asociado con el usuario, o bien una imagen que se ha validado previamente por el sistema de procesamiento 310 como una imagen del usuario), puede realizarse una comprobación para verificar que la segunda imagen 200 es una imagen de una persona real (un usuario “vivo”) en lugar de por ejemplo una fotografía estática de la persona.

Una comprobación de este tipo puede comprender las etapas de capturar una serie de imágenes del usuario del dispositivo 300, y comparar imágenes sucesivas para buscar diferencias entre imágenes sucesivas que indiquen que las imágenes son imágenes de un usuario vivo. Una vez que se han tomado dos imágenes sucesivas que son suficientemente diferentes para indicar que las imágenes son imágenes de un usuario vivo, el sistema de

procesamiento 310 puede usar una de estas imágenes como la segunda imagen 200 en un proceso de comparación como se ha descrito anteriormente.

Llevando a cabo una comprobación de este tipo se evitaría que un usuario de un dispositivo 300 se autentique a sí mismo como un usuario diferente sujetando una fotografía del usuario diferente delante del componente de captura de imagen 320.

En una disposición, antes de realizar una comparación entre dos imágenes sucesivas capturadas para buscar diferencias entre estas imágenes, las imágenes pueden analizarse para determinar porciones de la imagen que representan una cara humana, y porciones de la imagen que representan el fondo (pueden usarse conjuntos de imágenes de entrenamiento para un análisis de este tipo, como se ha descrito anteriormente). En esta disposición, al menos una sección de una de las imágenes que se determina que incluye tanto rasgos faciales como rasgos de fondo puede compararse a una sección correspondiente de la otra imagen para buscar movimiento de la cara con respecto al fondo. Una comparación de este tipo puede hacerse en una base píxel a píxel.

Como alternativa o adicionalmente, al menos una sección de una de las imágenes que se determina que incluye rasgos faciales únicamente se compara a una sección correspondiente de la otra imagen. Una comparación de este tipo puede buscar diferencias entre las imágenes indicativas de movimiento facial, tal como parpadeo.

Pueden compararse pares de imágenes capturadas posteriormente hasta que se identifique un par de imágenes capturadas posteriormente que son suficientemente diferentes para indicar que las imágenes son imágenes de un usuario vivo, o hasta que se haya comparado un número predeterminado de pares de imágenes capturadas posteriormente. Como alternativa, pueden compararse pares de imágenes capturadas posteriormente hasta que haya transcurrido un tiempo predeterminado.

Como se ha mencionado anteriormente, con referencia a la Figura 3 en particular, en una disposición, al menos parte del sistema de procesamiento 310 puede estar remoto del dispositivo 300. La Figura 7 muestra esquemáticamente un sistema de procesamiento remoto ejemplar 310 en una disposición de este tipo. El sistema de procesamiento 310 está conectado de manera comunicativa a una pluralidad de dispositivos, habiendo dos (300 y 300*) de tales dispositivos mostrados en la Figura 7.

En un ejemplo, un usuario de uno primero de los dos dispositivos 300 inicia un evento de autenticación de usuario en el primer dispositivo 300 a través de lo cual provoca que el primer dispositivo 300 capture una imagen del usuario del primer dispositivo 300. El primer dispositivo 300 puede capturar también una imagen 100 de un documento de identidad 110 asociado con un usuario 210, como se ha analizado anteriormente. En esta disposición, el primer dispositivo 300 a continuación envía dos imágenes capturadas 100, 200 al sistema de procesamiento 310, y tras la recepción, el sistema de procesamiento 310 determina si las dos imágenes 100, 200 son imágenes del mismo usuario. El sistema de procesamiento 310 puede llevar a cabo las etapas como se muestra en la Figura 4 para determinar si las imágenes representan el mismo usuario.

El primer dispositivo 300 puede recuperar también de manera opcional datos desde un chip del documento de identidad 110 y puede enviar estos datos recuperados al sistema de procesamiento 310.

El evento de autenticación puede asociarse con un identificador de evento de autenticación. El identificador puede generarse mediante el sistema de procesamiento 310 o el primer dispositivo 300, pero en cualquier caso, el identificador de evento de autenticación se comparte entre los dos componentes 300, 310 a través de lo cual identificar el evento de autenticación en los dos componentes 300, 310.

Una vez que el sistema de procesamiento 310 ha determinado si las imágenes representan el mismo usuario, el sistema de procesamiento 310 puede enviar una indicación al primer dispositivo 300, para confirmar el resultado del evento de autenticación, junto con el identificador de evento de autenticación, a través de lo cual indicar al primer dispositivo 300 si el usuario del primer dispositivo 300 es el usuario 210 representado en el documento de identidad 110 para ese evento de autenticación.

En la disposición donde el primer dispositivo 300 envía datos recuperados desde un chip del documento de identidad 110 al sistema de procesamiento 310, antes de confirmar el resultado del evento de autenticación al primer dispositivo 300, el sistema de procesamiento 310 puede usar los datos recuperados desde el chip para realizar comprobaciones adicionales. En particular, cuando los datos recuperados desde el chip comprenden una imagen del usuario asociado con el documento de identidad 110, el sistema de procesamiento puede comparar esta imagen a una o ambas de la primera y segunda imágenes 100, 200 como se ha descrito anteriormente. Esto es útil tanto al verificar la validez del documento de identidad 110, como también al aumentar la fiabilidad del resultado de autenticación.

En una disposición alternativa, cuando el sistema de procesamiento 310 ha autenticado previamente el usuario 210, el sistema de procesamiento 310 puede ya tener una o más imágenes validadas 200**, 200*** del usuario 210 almacenadas en un dispositivo de almacenamiento 600. En este caso, por lo tanto, el primer dispositivo 300 puede

no enviar una imagen 100 de un documento de identidad 110 asociado con el usuario 210 al sistema de procesamiento 310, pero puede en su lugar enviar detalles que identifican al usuario al sistema de procesamiento 210 que pueden usarse mediante el sistema de procesamiento 310 para identificar al usuario 210 y recuperar una imagen validada del usuario 210 desde el dispositivo de almacenamiento 600.

Como se ha analizado anteriormente, en una disposición, el sistema de procesamiento 310 puede almacenar imágenes validadas 200**, 200*** del usuario 210 junto con un identificador de usuario 610 para el usuario 210. En esta disposición, los detalles enviados desde el primer dispositivo 300 al sistema de procesamiento 310 pueden comprender el identificador de usuario 610 para el usuario 210, o como alternativa, los detalles pueden comprender detalles de los cuales puede derivarse el identificador de usuario 610. Este último caso es aplicable, por ejemplo, cuando el identificador de usuario 610 es un valor de troceo como se ha analizado anteriormente con referencia a la Figura 6.

Una vez que una imagen validada 200**, 200*** del usuario 210 se ha recuperado desde el dispositivo de almacenamiento 600, el sistema de procesamiento 310 compara la imagen 200 del usuario del primer dispositivo 300, que se recibió desde el primer dispositivo 300, a una imagen previamente validada 200**, 200*** del usuario 210 a través de lo cual verificar si el usuario del dispositivo 300 es el usuario previamente autenticado 210.

De nuevo, el evento de autenticación puede asociarse con un identificador de evento de autenticación, y el sistema de procesamiento 310 puede indicar el resultado de autenticación, junto con el identificador de evento de autenticación, al primer dispositivo 300.

Como se apreciará, los usuarios típicamente tienen más de un dispositivo, cada uno de los cuales tiene los medios para capturar imágenes. Por consiguiente, la imagen 100 del documento de identidad 110, puede capturarse mediante el segundo dispositivo 300*, mientras el primer dispositivo 300 se usa para tomar una imagen del usuario “vivo”. Esto puede ser útil si, por ejemplo, el segundo dispositivo 300* puede capturar imágenes que son de una calidad superior a las imágenes capturadas mediante el primer dispositivo 300. En esta disposición el identificador de evento de autenticación anteriormente descrito puede proporcionarse a ambos dispositivos 300, 300* de modo que el sistema de procesamiento 310 puede identificar imágenes recibidas desde los dos dispositivos diferentes relacionadas con el mismo evento de autenticación.

Tras recibir las dos imágenes 100, 200, el sistema de procesamiento puede configurarse para verificar que las dos imágenes 100, 200, están asociadas con el mismo identificador de evento de autenticación antes de compararlas a través de lo cual determinar si representan el mismo usuario, de la manera anteriormente descrita.

Como se ha mencionado anteriormente, una imagen validada dada 200 de un usuario previamente autenticado 210 puede almacenarse en conjunto con detalles relacionados con el dispositivo que se usa para capturar la imagen en la que el usuario previamente autenticado 210 se validó a sí mismo. Por lo tanto, cuando un usuario previamente autenticado 210 tiene una pluralidad de dispositivos 300, 300*, y se autentica a sí mismo mediante la pluralidad de dispositivos 300,300*, una pluralidad de imágenes validadas 200**, 200*** del usuario 210 pueden almacenarse en un dispositivo de almacenamiento remoto 600.

En una disposición, en un evento de autenticación posterior para el usuario previamente autenticado 210, el sistema de procesamiento 310 puede seleccionar una imagen previamente validada 200**, 200*** del usuario previamente autenticado 210 desde el dispositivo de almacenamiento 600 al menos en dependencia del identificador de dispositivo único del dispositivo en el que el usuario previamente autenticado 210 desea autenticarse a sí mismo (es decir el dispositivo de “autenticación”). Como un ejemplo, el sistema de procesamiento 310 puede seleccionar una imagen previamente validada 200**, 200*** del usuario 210 que se capturó mediante el dispositivo de autenticación para validar el usuario del dispositivo de autenticación. Esto puede mejorar la fiabilidad de los resultados de coincidencia facial, puesto que las dos imágenes a comparar es probable que sean similares, ya que se capturaron mediante el mismo dispositivo. El sistema de procesamiento 310 puede determinar también cuáles de las imágenes validadas previamente almacenadas 200**, 200*** usar cuando se valida el usuario en dependencia de las calidades de imagen designadas de las imágenes, como se ha analizado anteriormente. Por ejemplo, el sistema de procesamiento 310 puede usar una imagen previamente validada 200**, 200*** que se capturó mediante un dispositivo diferente del dispositivo de autenticación si es de calidad significativamente superior a una imagen validada que se capturó mediante el dispositivo de autenticación.

En relación con el aspecto de la invención donde las imágenes validadas se almacenan en un dispositivo de almacenamiento 600, el sistema de procesamiento 310 puede configurarse para evaluar las calidades de imagen de cada imagen validada y puede almacenar una asociación entre estas imágenes y sus calidades de imagen determinadas. En un evento de autenticación posterior, el sistema de procesamiento 310 puede seleccionar la imagen de la calidad más alta desde el dispositivo de almacenamiento 600 y comparar esta a una imagen del usuario de un dispositivo a través de lo cual autenticar a ese usuario. Como alternativa, el sistema de procesamiento 310 puede almacenar únicamente una imagen capturada si es de calidad superior a la imagen validada de un usuario previamente autenticado con la que se compara. Si la imagen capturada es de calidad superior, el sistema

de procesamiento 310 puede sustituir la imagen previamente validada por la imagen capturada, de manera que únicamente una imagen validada de un usuario dado se almacena en cualquier momento.

Aunque al menos algunos aspectos de las realizaciones descritas en el presente documento con referencia a los dibujos comprenden procesos informáticos realizados en sistemas o procesadores de procesamiento, la invención también se extiende a programas informáticos, particularmente programas informáticos en un soporte, adaptados para poner la invención en práctica. El programa puede estar en forma de código fuente no transitorio, código objeto, un código fuente intermedio y código objeto tal como en una forma parcialmente compilada, o en cualquier otra forma no transitoria adecuada para su uso en la implementación de procesos de acuerdo con la invención. El soporte puede ser cualquier entidad o dispositivo que pueda llevar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una unidad de estado sólido (SSD) u otra RAM basada en semiconductores; una ROM, por ejemplo un CD ROM o una ROM de semiconductores; un medio de grabación magnético, por ejemplo un disco flexible o disco duro; dispositivos de memoria óptica en general; etc.

Se entenderá que el sistema de procesamiento referenciado en el presente documento puede proporcionarse en la práctica mediante un único chip o circuito integrado o varios chips o circuitos integrados, proporcionados opcionalmente como un conjunto de chips, un circuito integrado específico de la aplicación (ASIC), campo de matriz de puertas programables (FPGA), procesador de señales digitales (DSP), etc. El chip o chips pueden comprender circuitería (así como posiblemente firmware) para realizar al menos uno de un procesador o procesadores de datos, un procesador o procesadores de señales digitales, circuitería de banda base y circuitería de frecuencia de radio, que son configurables para operar de acuerdo con las realizaciones ejemplares. En este sentido, las realizaciones ejemplares pueden implementarse al menos en parte mediante software informático almacenado en memoria (no transitoria) y ejecutarse mediante el procesador, o mediante hardware, o mediante una combinación de software y hardware tangiblemente almacenado (y firmware tangiblemente almacenado).

REIVINDICACIONES

1. Un método de determinación de si un usuario (210) de un dispositivo móvil (300) corresponde a un usuario previamente autenticado, habiéndose autenticado previamente el usuario (210) mediante un documento de identidad (110) que comprende: una imagen fotográfica (120) del usuario previamente autenticado, siendo visible la imagen fotográfica (120) en dicho documento de identidad (110); y un componente de circuito integrado que almacena datos representativos de una imagen digital del usuario previamente autenticado, comprendiendo el método:

provocar que un lector de chips conectado a o integral con el dispositivo móvil (300) acceda al componente de circuito integrado, a través de lo cual recuperar dichos datos representativos de una imagen digital del usuario previamente autenticado;
provocar que una cámara (320) conectada a o integral con el dispositivo móvil (300) capture una primera imagen (100), correspondiendo la primera imagen (100) a una imagen de una porción del documento de identidad (110) que contiene dicha imagen fotográfica (120) visible en el documento de identidad (110);
provocar que una cámara (320) conectada a o integral con el dispositivo móvil (300) capture una segunda imagen (200), correspondiendo la segunda imagen (200) a un usuario (210) del dispositivo móvil (300); y,
disponer que dichos datos recuperados y datos indicativos de dicha primera y segunda imágenes (100, 200) se comparen, a través de lo cual determinar si la primera imagen (100), la segunda imagen (200) y la imagen digital representan el mismo usuario (210); y,
en el caso de que se determine que la primera imagen (100), la segunda imagen (200) y la imagen digital representan el mismo usuario (210), formar una asociación entre el usuario previamente autenticado y el dispositivo móvil (300), en el que la asociación verifica el dispositivo móvil (300) como un dispositivo móvil del usuario previamente autenticado.

2. Un método de acuerdo con la reivindicación 1, que comprende disponer que los datos recuperados y los datos indicativos de la primera imagen (100) se comparen, a través de lo cual verificar la validez del documento de identidad (110).

3. Un método de acuerdo con la reivindicación 2, en el que el documento de identidad (110) comprende adicionalmente primeros datos, y el método comprende adicionalmente disponer que los primeros datos se deriven del documento de identidad (110) y que se realice dicha verificación de la validez del documento de identidad basándose en los primeros datos.

4. Un método de acuerdo con la reivindicación 3, en el que al menos algunos de dichos primeros datos se almacenan en el componente de circuito integrado, y la etapa de disponer que los primeros datos se deriven del documento de identidad comprende provocar que un lector de chips conectado a o integral con el dispositivo móvil (300) acceda al componente de circuito integrado para recuperar dichos primeros datos.

5. Un método de acuerdo con la reivindicación 3 o la reivindicación 4, en el que al menos algunos de dichos primeros datos son visibles en dicho documento de identidad (110), y dicha primera imagen (100) comprende una porción del documento de identidad (110) que contiene dichos primeros datos, y en el que la etapa de disponer que los primeros datos se deriven del documento de identidad (110) comprende: o bien analizar rasgos en dicha primera imagen (100), o bien enviar dicha primera imagen (100) a un sistema de procesamiento remoto que está configurado para analizar rasgos en dicha primera imagen (100), a través de lo cual derivar del documento de identidad (110) dichos primeros datos.

6. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en el que el documento de identidad (110) comprende adicionalmente segundos datos relacionados con el usuario previamente autenticado, y el método comprende adicionalmente disponer que dichos segundos datos se deriven del documento de identidad (110), y que se almacenen dichos segundos datos derivados, junto con un identificador para el usuario previamente autenticado.

7. Un método de acuerdo con la reivindicación 6, en el que al menos algunos de dichos segundos datos se almacenan en el componente de circuito integrado, y dicha etapa de disponer que dichos segundos datos se deriven del documento de identidad (110) comprende provocar que un lector de chips conectado a o integral con el dispositivo móvil (300) acceda al componente de circuito integrado, a través de lo cual recuperar dichos segundos datos.

8. Un método de acuerdo con la reivindicación 6 o la reivindicación 7, en el que al menos algunos de dichos segundos datos son visibles en dicho documento de identidad (110), y dicha primera imagen (100) comprende una porción del documento de identidad (110) que contiene dichos segundos datos, y en el que la etapa de disponer que dichos segundos datos se deriven del documento de identidad (110) comprende disponer que dichos segundos datos se extraigan de la primera imagen (100) usando reconocimiento óptico de caracteres.

9. Un método de acuerdo con la reivindicación 3 y la reivindicación 6, en el que los segundos datos son un subconjunto de los primeros datos.

10. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 9, en el que dicha etapa de disponer la comparación de los datos representativos de una imagen digital del usuario previamente autenticado y los datos indicativos de la primera y segunda imágenes (100, 200) comprende enviar los datos representativos de una imagen digital del usuario previamente autenticado y los datos indicativos de dicha primera y segunda imágenes (100, 200) a un sistema de procesamiento remoto (310) configurado para llevar a cabo dicha comparación.

11. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 10, en el que los datos representativos de una imagen digital del usuario previamente autenticado y los datos indicativos de dicha primera y segunda imágenes (100, 200) se comparan mediante un sistema de procesamiento (310) del dispositivo móvil (300).

12. Un sistema de procesamiento (310) para su uso en la determinación de si un usuario (210) de un dispositivo móvil (300) corresponde a un usuario previamente autenticado, habiéndose autenticado previamente el usuario (210) mediante un documento de identidad (110) que comprende: una imagen fotográfica (120) del usuario previamente autenticado, siendo visible la imagen fotográfica (120) en dicho documento de identidad (110); y un componente de circuito integrado que almacena datos representativos de una imagen digital del usuario previamente autenticado, estando configurado el sistema de procesamiento (310) para:

provocar que un lector de chips conectado a o integral con el dispositivo móvil (300) acceda al componente de circuito integrado, a través de lo cual recuperar dichos datos representativos de una imagen digital del usuario previamente autenticado;
provocar que una cámara (320) conectada a o integral con el dispositivo móvil (300) capture una primera imagen (100), correspondiendo la primera imagen (100) a una imagen de una porción del documento de identidad (110) que contiene dicha imagen fotográfica (120) visible en el documento de identidad (110);
provocar que una cámara (320) conectada a o integral con el dispositivo móvil (300) capture una segunda imagen (200), correspondiendo la segunda imagen (200) a un usuario (210) del dispositivo móvil (300);
disponer que dichos datos recuperados y datos indicativos de dicha primera y segunda imágenes (100, 200) se comparen, a través de lo cual determinar si la primera imagen (100), la segunda imagen (200) y la imagen digital representan el mismo usuario; y,
en el caso de que se determine que la primera imagen (100), la segunda imagen (200) y la imagen digital representan el mismo usuario, formar una asociación entre el usuario previamente autenticado y el dispositivo móvil (300), en el que la asociación verifica el dispositivo móvil (300) como un dispositivo móvil del usuario previamente autenticado.

13. Un sistema de procesamiento (310) de acuerdo con la reivindicación 12, en el que el sistema de procesamiento (310) está configurado para disponer que los datos recuperados y los datos indicativos de la primera imagen (100) se comparen, a través de lo cual verificar la validez del documento de identidad (110).

14. Un sistema de procesamiento (310) de acuerdo con la reivindicación 12 o 13, en el que el sistema de procesamiento (310) está configurado para provocar que el lector de chips utilice un protocolo de comunicación de campo cercano para acceder al componente de circuito integrado.

15. Un programa informático para su uso en la determinación de si un usuario (210) de un dispositivo móvil (300) corresponde a un usuario previamente autenticado, habiéndose autenticado previamente el usuario (210) mediante un documento de identidad (110) que comprende: una imagen fotográfica (120) del usuario previamente autenticado, siendo visible la imagen fotográfica (120) en dicho documento de identidad (110); y un componente de circuito integrado que almacena datos representativos de una imagen digital del usuario previamente autenticado, y comprendiendo el programa informático instrucciones de manera que, cuando el programa informático se ejecuta en un sistema de procesamiento, el sistema de procesamiento está configurado para llevar a cabo un método de acuerdo con cualquiera de las reivindicaciones 1 a 11.

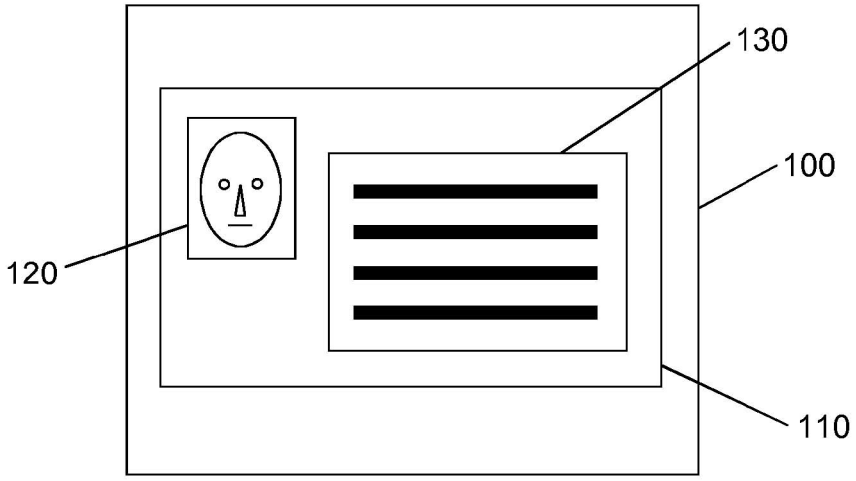

Fig. 1

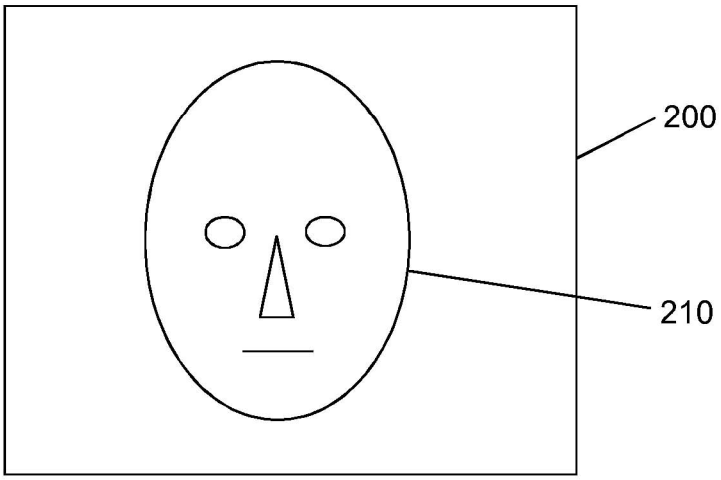

Fig. 2

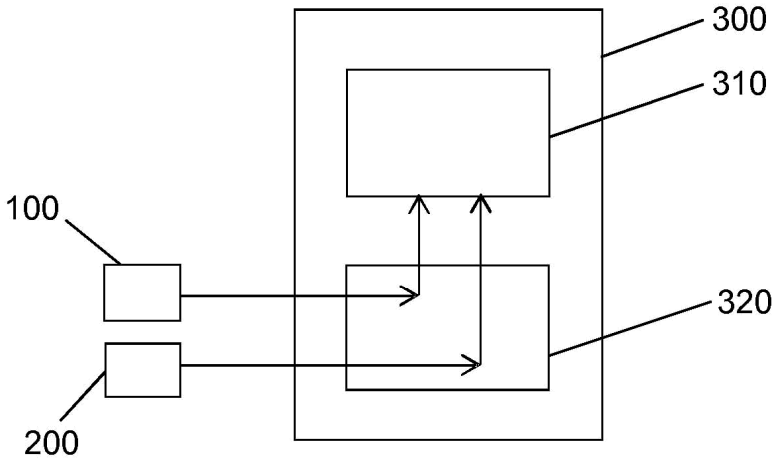
300
310
100
320
200

Fig. 3

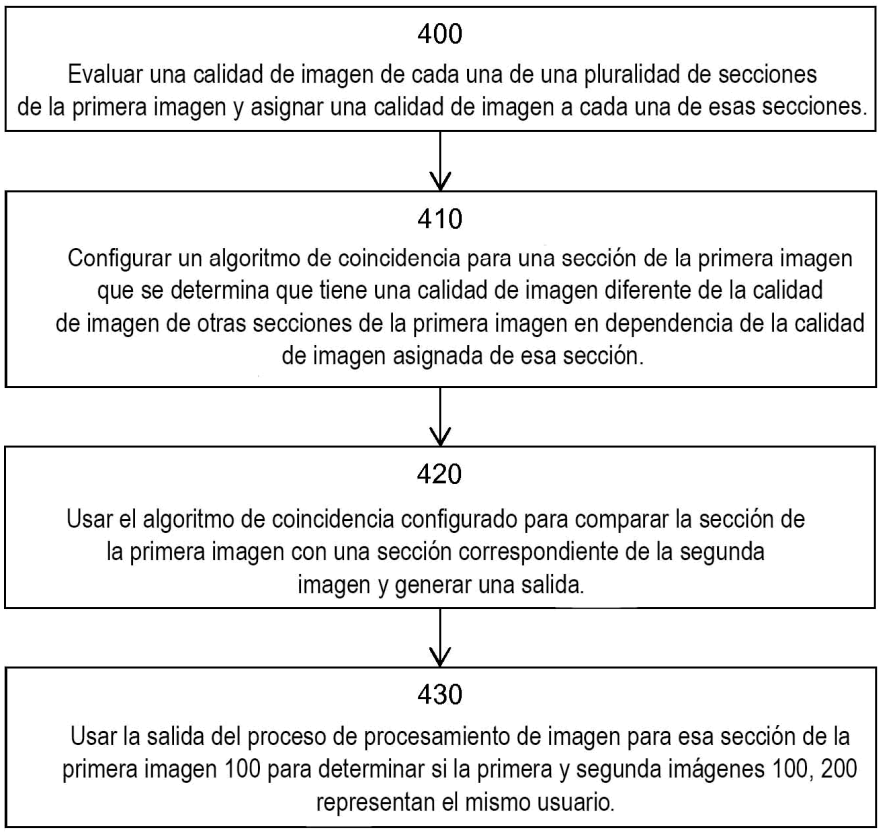
400
Evaluar una calidad de imagen de cada una de una pluralidad de secciones de la primera imagen y asignar una calidad de imagen a cada una de esas secciones.
410
Configurar un algoritmo de coincidencia para una sección de la primera imagen que se determina que tiene una calidad de imagen diferente de la calidad de imagen de otras secciones de la primera imagen en dependencia de la calidad de imagen asignada de esa sección.
420
Usar el algoritmo de coincidencia configurado para comparar la sección de la primera imagen con una sección correspondiente de la segunda imagen y generar una salida.
430
Usar la salida del proceso de procesamiento de imagen para esa sección de la primera imagen 100 para determinar si la primera y segunda imágenes 100, 200 representan el mismo usuario.

Fig. 4

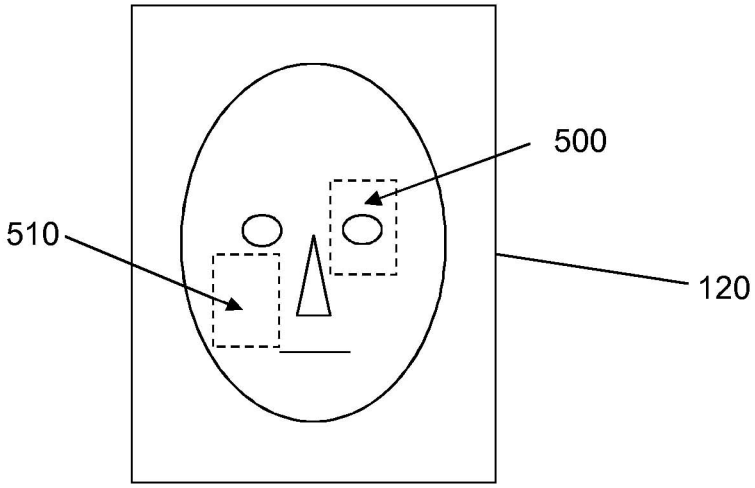

Fig. 5

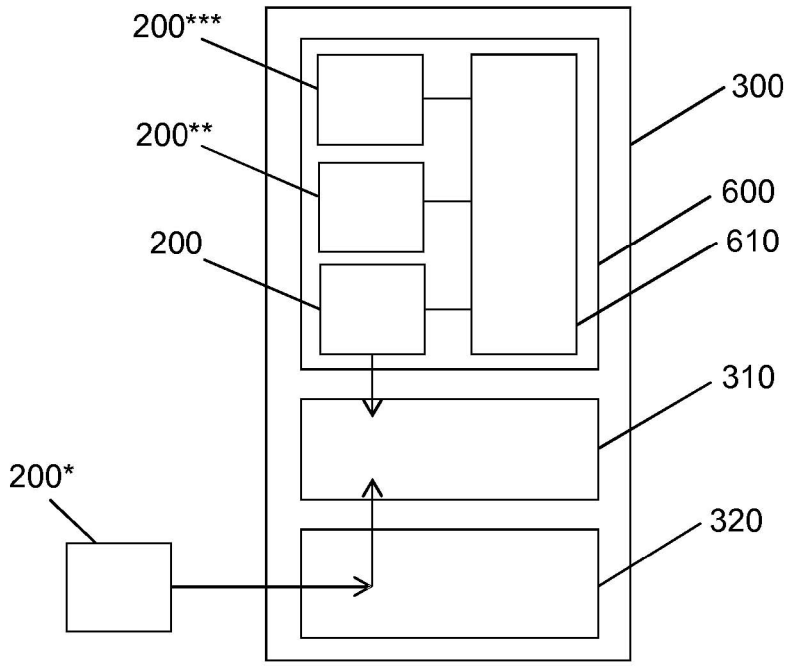

Fig. 6

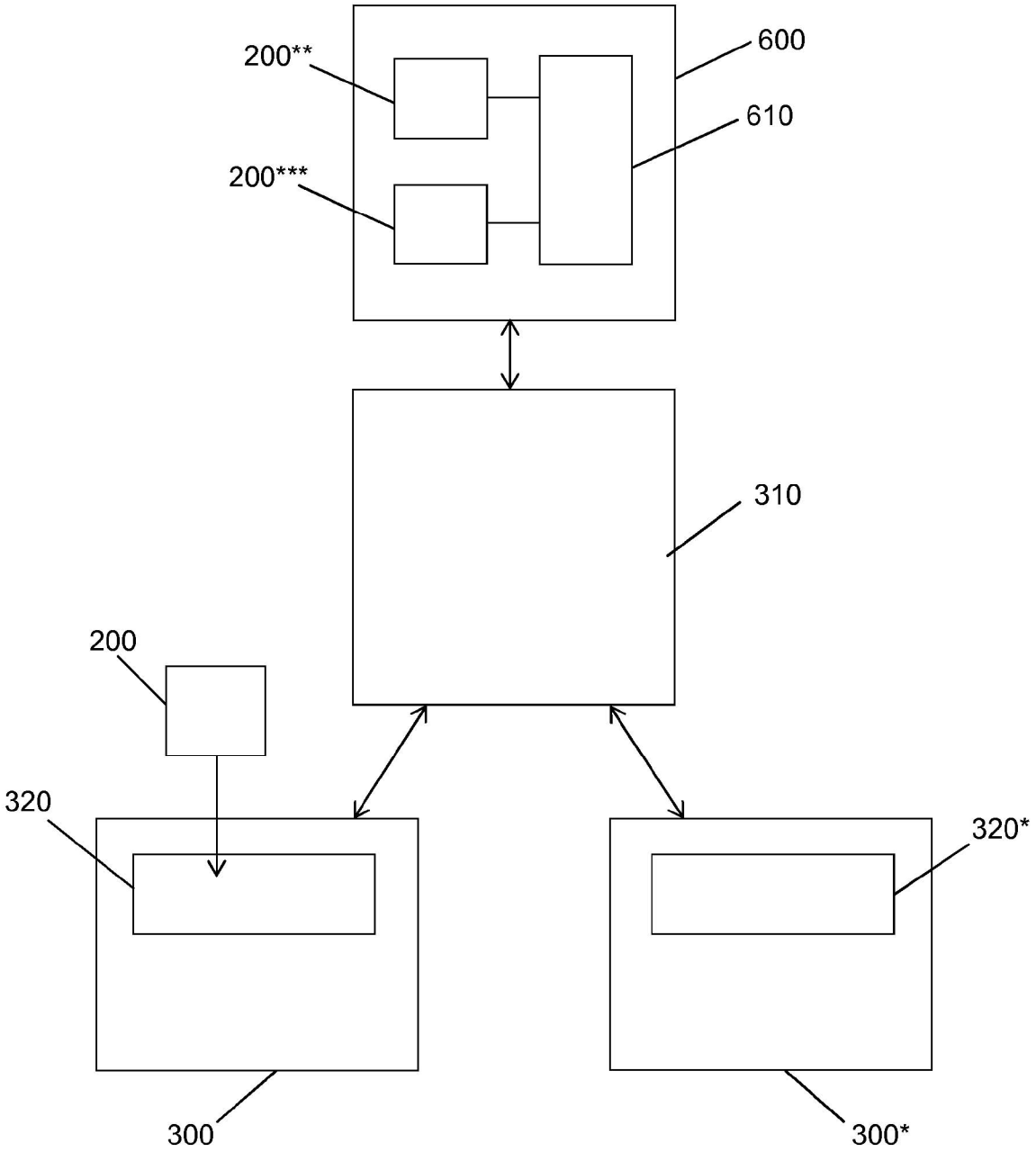

Fig. 7