(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 535 415**

(51) Int. CI.:

G06F 21/31 (2013.01)
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.11.2011 E 11801791 (2)**

(97) Fecha y número de publicación de la concesión europea: **07.01.2015 EP 2656321**

(54) Título: **Procedimiento para permitir una autenticación o una identificación de un individuo y sistema de verificación asociado**

(30) Prioridad:

23.12.2010 FR 1061160

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2015

(73) Titular/es:

MORPHO (100.0%)
11 Boulevard Gallieni
92130 Issy-les-Moulineaux, FR

(72) Inventor/es:

FONDEUR, JEAN-CHRISTOPHE y
CHABANNE, HERVÉ

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento para permitir una autenticación o una identificación de un individuo y sistema de verificación asociado

La presente invención concierne a la autenticación o la identificación (es decir una verificación) de un individuo con la ayuda de un dispositivo electrónico.

Se observará que, en el conjunto del presente texto, cuando se hable de autenticación o de identificación, el "o" es inclusivo, es decir que significa "y/o", de modo que la presente invención es aplicable tanto a la autenticación como a la identificación, incluso a las dos a la vez.

La autenticación o la identificación utilizan tradicionalmente un servidor que almacena datos relativos a individuos que previamente hayan sido objeto de una fase denominada de registro (o de inscripción) en el citado servidor para obtener, con la autenticación o la identificación, un derecho cualquiera (expedición de un permiso de conducir, de un título de transporte, de una indemnización, autorización de acceso a un local, autorización de acceso a un servicio, puesta en práctica de un servicio, pago electrónico, etc).

Los datos utilizados tradicionalmente para el registro de individuos en el servidor son datos personales, generalmente alfanuméricos, tales como contraseñas, direcciones de dispositivos electrónicos utilizadas por los individuos (es decir IP), identidades y /u otros.

Para ser suficientemente discriminantes y así permitir una autenticación o una identificación con una tasa de éxitos aceptable, los datos utilizados pueden ser relativamente complejos desde el punto de vista de los individuos. A título de ejemplo, cuantos más caracteres contenga una contraseña, más fiable podrá ser una autenticación o una identificación, pero más difícil será su memorización por un individuo.

Para aligerar la tarea de los individuos, se ha propuesto basar el registro y la autenticación o la identificación con otros tipos de datos, tales como imágenes predeterminadas, en sustitución o como complemento de los datos tradicionales.

Así, durante un registro, un individuo es llevado a elegir un número reducido de imágenes entre un conjunto finito de imágenes predeterminadas. A título ilustrativo, el individuo puede elegir un tema en una lista (una raza animal, un tipo de diversión, etc), y seleccionar una imagen relativa al tema elegido entre algunas decenas o centenares de imágenes propuestas. A continuación, la autenticación o la identificación pueden consistir, para este individuo, en reproducir el mismo esquema y así volver a seleccionar la misma imagen, de modo que esta última sea comparada con la imagen seleccionada durante el registro.

En caso de identidad entre las dos imágenes, eventualmente como complemento de una comparación entre otros tipos de datos, se puede deducir que el individuo considerado corresponde a un individuo alistado (caso de una identificación) o al individuo que pretende ser alistado (caso de una autenticación).

Este proceso, si bien evita al individuo tener que memorizar datos demasiado complejos, requiere todavía un esfuerzo no despreciable por parte del individuo para seleccionar las imágenes y retener su selección entre el registro y cada autenticación o identificación.

Además, siendo necesariamente de tamaño limitado el conjunto de las imágenes predeterminadas propuestas a cada individuo, la probabilidad de que dos individuos elijan la o las mismas imágenes puede ser elevada, limitando así la fiabilidad de la autenticación o la identificación.

El documento WO02/37429 divulga otro procedimiento de autenticación a base de contraseña gráfica.

Un objetivo de la presente invención es aligerar todavía un poco más la tarea de los individuos y, en su caso, permitir una mejora del rendimiento de la autenticación o la identificación.

La invención propone así un procedimiento para permitir la autenticación o la identificación de un individuo con la ayuda de un primer dispositivo electrónico que comprende una unidad de captura de imagen y una unidad de transmisión de datos, incluyendo el procedimiento una fase de registro del citado individuo en un sistema de verificación (es decir de autenticación o de identificación). La fase de registro comprende las etapas siguientes:

- captura de una primera imagen de al menos un objeto cualquiera elegido secretamente por el individuo, con la ayuda de la unidad de captura de imagen del citado primer dispositivo electrónico;

- transmisión, con la ayuda de la unidad de transmisión de datos del citado primer dispositivo electrónico, de la citada primera imagen al sistema de verificación.

De este modo, la complejidad es transferida del individuo al sistema de verificación. En efecto, siendo obtenida la imagen completamente a su idea por el individuo que elige libremente un objeto o una parte de un objeto que hay que fotografiar, se obtiene un nivel de personalización verdaderamente notable, susceptible de reducir el esfuerzo de memorización del citado individuo. A la inversa, el algoritmo de comparación de imágenes que hay que poner en

práctica por el sistema de verificación para la autenticación o la identificación puede ser relativamente complejo con respecto a los algoritmos de comparación de datos más tradicionales (como la comparación entre dos contraseñas o entre dos imágenes conocidas de antemano).

Además, siendo obtenida la imagen por el individuo entre un conjunto no determinado de antemano y potencialmente infinito, se reduce el riesgo de ver a dos individuos adquirir la misma imagen o imágenes muy similares, lo que puede mejorar el rendimiento de la autenticación o la identificación con respecto a la técnica anterior mencionada anteriormente y/o reducir el recurso a otros tipos de datos complejos como complemento de las imágenes.

En modos de realización ventajosos que pueden ser combinados de todas las maneras posibles:

- el objeto elegido por el individuo es un objeto que el individuo tiene siempre o está a su alcance. Se simplifica entonces la tarea del individuo, porque su autenticación o identificación puede hacerse con menor esfuerzo, y eventualmente en cualquier lugar y/o cualquier momento;

- la primera imagen es transmitida al sistema de verificación de modo protegido. Se evita así que un atacante pueda capturarla en el transcurso de la transmisión. La transmisión, protegida o no, de la primera imagen al sistema de verificación puede ser directa o transitar por uno o varios equipos intermedios;

- al menos un primer dato personal del citado individuo es transmitido al sistema de verificación como complemento de la primera imagen. Se enriquecen así los tipos de datos que permitirán la autenticación o la identificación;

- el procedimiento incluye además una fase de autenticación o de identificación relativa al citado individuo con la ayuda de un segundo dispositivo electrónico, comprendiendo la fase de autenticación o de identificación las etapas siguientes puestas en práctica a nivel del sistema de verificación:

    - recepción desde el segundo dispositivo electrónico de una segunda imagen de al menos un objeto idéntico o similar al de la primera imagen;

    - comparación de la segunda imagen al menos con la primera imagen;

    - conclusión de que el individuo está autenticado o identificado con éxito cuando la comparación de la segunda imagen con la primera imagen revela una concordancia entre sus respectivos objetos.

- el procedimiento comprende además la recepción desde el segundo dispositivo electrónico de un segundo dato personal del citado individuo correspondiente al primer dato personal y la comparación del segundo dato personal al menos con el primer dato personal, y en el cual se concluye que el individuo es autenticado o identificado con éxito cuando la comparación de la segunda imagen con la primera imagen revela una concordancia entre sus respectivos objetos y la comparación del segundo dato personal con el primer dato personal revela una concordancia entre el segundo dato personal y el primer dato personal.

- la segunda imagen ha sido capturada fácilmente con la ayuda de una unidad de captura de imagen del citado segundo dispositivo electrónico, a los fines de la autenticación o de la identificación del individuo en el citado sistema de verificación. Se evita así un almacenamiento y una reutilización de la primera imagen que se considerarían menos seguros.

- el primer dispositivo electrónico y el segundo dispositivo electrónico son un mismo dispositivo.

- el primer dispositivo electrónico y/o el segundo dispositivo electrónico pertenecen al citado individuo. Se simplifica así de nuevo la tarea del individuo. Puede tratarse por ejemplo de un teléfono móvil u otro que el individuo lleve habitualmente consigo o al cual tenga fácilmente acceso.

- la segunda imagen es transmitida al sistema de verificación desde el segundo dispositivo electrónico de modo protegido. Se evita así que un atacante pueda capturarla en el transcurso de la transmisión. La transmisión, protegida o no, de la segunda imagen al sistema de verificación puede ser directa o y transitar por uno o varios equipos intermedios.

La invención propone además un sistema de verificación para permitir la autenticación o la identificación de un individuo de acuerdo con el procedimiento antes mencionado. El sistema de verificación comprende

- una primera unidad de recepción para recibir, desde un primer dispositivo electrónico, una primera imagen capturada de al menos un objeto cualquiera elegido secretamente por el individuo;

- una segunda unidad de recepción (que eventualmente es la misma que la primera unidad de recepción) para recibir, desde un segundo dispositivo electrónico, una segunda imagen de al menos un objeto idéntico o similar al de la primera imagen;

- un comparador de imágenes para comparar la segunda imagen al menos con la primera imagen;

- una señal de decisión para concluir que el individuo está autenticado o identificado con éxito cuando la comparación de la segunda imagen con la primera imagen efectuada por el comparador revela una concordancia entre sus respectivos objetos.

El sistema de verificación puede consistir en un dispositivo único (es decir un servidor), o bien puede estar distribuido entre varias entidades. A título de ejemplo no limitativo, las unidades de recepción y el comparador de imágenes podrían formar parte de una primera entidad, por ejemplo colocalizada o situada en la proximidad del dispositivo electrónico, mientras que la unidad de decisión podría recurrir a una segunda entidad distinta de la primera, por ejemplo de tipo servidor centralizado.

La invención propone también un producto programa de ordenador que comprenda instrucciones de código para poner en práctica el procedimiento antes mencionado, cuando éste esté cargado y sea ejecutado con medios informáticos, por ejemplo del primer dispositivo electrónico y/o del segundo dispositivo electrónico y/o de sistema de verificación.

Otras particularidades y ventajas de la presente invención se pondrán de manifiesto en la descripción que sigue de ejemplos de realización no limitativos, refiriéndose a los dibujos anejos, en los cuales:

- la figura 1 es un esquema que muestra un ejemplo de una fase de registro que puede ser puesta en práctica de acuerdo con un modo de realización de la invención;

- la figura 2 es un esquema que muestra un ejemplo de una fase de autenticación o de identificación que puede ser puesta en práctica de acuerdo con un modo de realización de la invención.

Un primer aspecto de la invención consiste en una fase de registro (o de inscripción) de un individuo en un sistema de verificación, con miras a una eventual autenticación o identificación posterior del citado individuo. Como se indicó anteriormente, esta fase de registro tiene por objetivo, para el individuo, proveerse posteriormente de un derecho cualquiera (expedición de un permiso de conducir, de un título de transporte, de una indemnización, autorización de acceso a un local, autorización de acceso a un servicio, puesta en práctica de un servicio, pago electrónico, etc.).

Este aspecto está ilustrado en el ejemplo no limitativo en la figura 1, en el cual el individuo 1 se registra en un sistema de verificación 3, que puede ser de cualquier tipo concebible. A título de ejemplo puede tratarse de un servidor de forma cualquiera (ordenador con memoria de almacenamiento local, sistema informático complejo que coopere con una memoria de almacenamiento distante, etc.). De acuerdo con otro ejemplo no limitativo, el sistema de verificación puede ser un sistema distribuido entre varias entidades, estando encargada cada una de una o varias funciones. Para simplificar la lectura de lo que sigue de la descripción, se considerará más particularmente el caso en el que el sistema de verificación 3 consista en un único servidor (se hablará entonces del servidor 3).

El registro es efectuado con la ayuda de un dispositivo electrónico 2 que comprende una unidad de captura de imagen y una unidad de transmisión de datos. Este dispositivo electrónico puede ser de cualquier tipo concebible. Puede tratarse por ejemplo de un dispositivo móvil tal como un teléfono móvil, un teléfono inteligente, un asistente personal numérico (PDA), un ordenador móvil, una tableta electrónica u otro, provisto de un módulo fotográfico y/o de video y que tenga medios de transmisión de datos de acuerdo con cualquier tecnología apropiada (transmisión de acuerdo con un estándar de comunicación celular tal como GPRS, EDGE, UMTS, LTE u otro, transmisión de acuerdo con una tecnología radio como Wifi, WiMax, Bluetooth, etc.).

En variante o como complemento, puede tratarse por ejemplo de un dispositivo fijo tal como un ordenador provisto de una webcam y de medios de transmisión de datos de acuerdo con un procedimiento de tipo IP u otro.

En variante o como complemento, puede tratarse, por una parte, de un dispositivo complejo que hace intervenir varias entidades separables, como un aparato fotográfico o una cámara de video para la captura de imagen y, por otra, de una entidad distinta como un ordenador u otro para la transmisión de datos. En este último caso, las diferentes entidades que constituyen el dispositivo deben ser capaces de cooperar de manera que una imagen capturada por una entidad pueda ser transmitida a continuación de manera apropiada por la otra entidad.

Ventajosamente, el dispositivo electrónico 2 es utilizado por el individuo 1 para su propio uso, o incluso le pertenece, es decir que es de la propiedad del individuo 1. Es particularmente ventajoso que el individuo 1 esté provisto del dispositivo electrónico 2 de modo habitual, como es el caso por ejemplo de un teléfono móvil, de manera que el individuo 1 pueda utilizarlo en cualquier momento o casi. Sin embargo, es posible que el dispositivo electrónico 2 no sea propiedad del individuo 1, sino que sea utilizado por varios, incluso por todos los individuos que sean objeto de una fase de registro. Así, puede tratarse de un dispositivo directamente asociado al servidor 3.

En el marco del registro del individuo 1, se captura una imagen I_1 con la ayuda de la unidad de captura de imagen del dispositivo electrónico 2 (etapa 4). Esta imagen I_1 representa uno o varios objetos O_1 cualesquiera elegidos secretamente por el individuo 1. En este contexto, el término “objeto” debe comprenderse en su acepción más amplia. La imagen I_1 puede ser así la de al menos un objeto físico. A título de ejemplo particularmente ventajoso, el

objeto O_1 representado en la imagen I_1 puede ser un elemento característico que el individuo 1 lleve siempre o generalmente consigo o esté a su alcance, como un llavero fetiche, una joya, una fotografía, un tatuaje, una cicatriz, u otro.

En variante, o como complemento, el objeto O_1 puede parecerse a otra cosa que un objeto físico, por ejemplo una escena característica, como una puesta de sol, u otro.

Se observará que la noción de imagen debe comprenderse también en un alcance amplio. A título de ejemplo, la imagen I_1 capturada puede ser una imagen fija o animada (es decir de video).

Cuantos más objetos O_1 represente la imagen I_1 (o un objeto O_1 raro), más discriminante será ésta y por tanto más fiable será la eventual autenticación o la identificación posterior. A título de ejemplo ilustrativo, si el objeto O_1 corresponde a una fotografía de un objeto raro, la imagen I_1 capturada de este objeto será relativamente discriminante.

En cualquier caso, el o los objetos O_1 representados en la imagen I_1 pueden ser cualesquiera, es decir que el individuo 1 es el que les elige libremente, sin estar en modo alguno obligado a elegir un conjunto predefinido o a partir de un soporte existente. A título de ejemplo, contrariamente a la técnica anterior mencionada en la introducción, el individuo 1 no tiene que elegir un objeto según temas o categorías predefinidas. Éste tampoco tiene que seleccionar una imagen entre un conjunto finito de imágenes que representen objetos predeterminados. Al contrario, el individuo 1 genera su propia imagen I_1, completamente a su idea. Debido a esto, el espacio posible de las imágenes es casi infinito y, en cualquier caso, de tamaño muy superior al de la mencionada técnica anterior.

Además, gracias a este fuerte poder de personalización durante la captura de la imagen I_1, el esfuerzo de memorización necesario para que el individuo pueda acordarse del objeto O_1 en un estado posterior puede ser considerablemente reducido, especialmente con respecto al ejercicio consistente en reconocer posteriormente una o varias imágenes entre algunas decenas o centenares de imágenes predeterminadas, eventualmente similares.

Otra ventaja de este modo de funcionamiento reside en el hecho de que solo el individuo 1 conoce el objeto O_1 de la imagen I_1 capturada, puesto que la elección de este objeto es efectuada secretamente por el individuo 1 (es decir sin informar de ello a nadie). En particular, el servidor 3 no conoce la naturaleza del objeto O_1 y no se hace ninguna clasificación de la imagen I_1 según un tipo de objeto O_1 que ésta represente. Debido a esto, el individuo 1 retiene un secreto que hace compleja la tarea de un atacante que deseara encontrar, en el servidor 3, un dato relativo al individuo 1. A título de ilustración, la potencia de cálculo que hay que poner en práctica por un atacante para comparar dos imágenes sin conocer de antemano el tipo de contenido no tiene punto de comparación con la -relativamente baja – requerida para comparar cadenas de una decena de caracteres alfanuméricos.

La imagen I_1 así adquirida es transmitida después al servidor 3 con la ayuda de la unidad de transmisión de datos del dispositivo electrónico 2 (etapa 5). Esta transmisión puede ser directa o bien transitar por uno o varios dispositivos intermedios, como por ejemplo en el caso en que la transmisión se haga a través de una red de comunicación.

El formato en el cual la imagen I_1 es transmitida puede ser cualquiera. Puede tratarse por ejemplo del formato directamente obtenido de la captura de imagen (por ejemplo JPEG, BMP, MPEG, u otro). En variante, puede utilizarse otro formato para la transmisión, por ejemplo el resultante de una compresión de imagen.

Ventajosamente, la transmisión 5 de la imagen I_1 con destino al servidor 3 es efectuada de modo protegido. A tal efecto, puede considerarse cualquier procedimiento apropiado de aseguramiento de la transmisión, como por ejemplo el recurso al protocolo HTTPS, SSL/TLS u otro. Se evita así que un atacante pasivo que vigile la vía de transmisión entre el dispositivo electrónico 2 y el servidor 3 pueda tener acceso en claro a la imagen I_1.

A la recepción de la imagen I_1, el servidor 3 la conserva ventajosamente en una memoria local o distante a la cual tenga acceso, con miras a encontrarla durante una eventual futura autenticación o identificación.

De modo ventajoso, uno o varios datos personales del individuo 1 pueden ser transmitidos al servidor 3 como complemento de la imagen I_1. Estos datos pueden ser transmitidos por ejemplo con la ayuda de la unida de transmisión de datos del dispositivo electrónico 2 o por cualquier otro medio apropiado. Estos datos personales pueden comprender cualesquiera datos susceptibles de ser utilizados en el marco de una autenticación o de una identificación. A título ilustrativo, estos pueden comprender al menos uno entre: una contraseña, una dirección electrónica del dispositivo electrónico 2, una identidad, u otro.

En este caso, los diferentes datos relativos al individuo 1 son ventajosamente almacenados en asociación por o para el servidor 3. Esto es lo que ilustra la figura 1, en la que la imagen I_1 es memorizada al lado de una contraseña m_1 del individuo 1 (referencia (I_1, m_1)).

Una ventaja del modo de registro que ha sido descrito hasta ahora reside en la facilidad, para el individuo 1, de revocarle. Esta revocación puede consistir en efecto en una simple supresión de la imagen I_1 a nivel del servidor 3,

por ejemplo después de una solicitud en este sentido que provenga del dispositivo electrónico 2 u otro. Para tal revocación puede considerarse igualmente una sustitución de la imagen I_1 por otra imagen, relativa al individuo 1.

Se observará igualmente que la utilización de la imagen I_1 garantiza el respeto de la vida privada del individuo 1, puesto que esta imagen solamente facilita información sobre el citado individuo. En particular, en general será difícil o incluso imposible encontrar la identidad del individuo 1 a partir de la sola imagen I_1.

Otra ventaja todavía es que el modo de registro que ha sido descrito hasta ahora solamente necesita una estructura simple y un material limitado. En efecto, como se mencionó anteriormente, el individuo 1 puede registrarse con la ayuda de un simple teléfono móvil equipado por ejemplo con un módulo fotográfico. El recurso a material especializado (tarjeta inteligente, módulo de tratamiento numérico específico, etc.) no es necesario, aunque éste tampoco se excluye. Esta facilidad, para el individuo 1 de registrarse a menor coste y esfuerzo, puede ser calificada de autorregistro.

Se describe ahora otro aspecto de la invención refiriéndose a la figura 2. Se trata de la fase de autenticación o de identificación de un individuo cualquiera. En el ejemplo que sigue, el interés se centra en el mismo individuo 1 que el que ha sido objeto previamente de un registro en el servidor 3 como se describió anteriormente.

En esta fase, se utiliza un dispositivo electrónico que puede ser el mismo que el utilizado para el registro o bien otro dispositivo electrónico. En el ejemplo no limitativo ilustrado en la figura 2, se utiliza el mismo dispositivo electrónico 2.

Una imagen I'_1 es obtenida por el dispositivo electrónico 2 (etapa 6) para ser transmitida al servidor 3 (etapa 7). Esta imagen I'_1 representa uno o varios objetos idénticos o similares al de o a los de la imagen I_1 capturada con ocasión del registro previo. En el presente ejemplo, la imagen I'_1 representa el mismo objeto O_1 que el de la imagen I_1. En variante, esta imagen podría representar un objeto O'_1 similar al objeto O_1 de la imagen I_1 variante. A título de ejemplo, si el objeto O_1 consiste en una escena dada, por ejemplo una puesta de sol, el objeto O'_1 podría consistir en una escena comparable aunque no idéntica, por ejemplo una puesta de sol fotografiada en otro lugar y/u otro día.

El modo en que la imagen I'_1 es obtenida por el dispositivo electrónico 2 puede ser diverso. Así, si la imagen I_1 ha sido memorizada por el dispositivo electrónico 2 con ocasión de la fase de registro, la misma imagen puede ser encontrada y de nuevo transmitida por el dispositivo electrónico 2 con fines de la autenticación o de la identificación. En este caso, la imagen I'_1 es estrictamente idéntica a la imagen I_1.

En variante o como complemento, la imagen I'_1 puede ser capturada recientemente con la ayuda de la unidad de captura de imagen del dispositivo electrónico 2 (o de cualquier otro dispositivo electrónico utilizado en esta fase) con fines de la autenticación o de la identificación del individuo 1 ante el servidor 3. Se entiende por « imagen recientemente capturada » una imagen no previamente registrada ni transmitida al sistema de verificación, es decir una imagen adquirida para las necesidades de la comparación en el momento de la autenticación o de la identificación del individuo. En esta hipótesis, el individuo 1 podrá ventajosamente esforzarse en capturar una imagen « reciente » I'_1 del objeto O_1 tan similar como sea posible a la imagen de referencia I_1 para facilitar la comparación de las dos imágenes por el servidor 3. Sin embargo, las imágenes I_1 e I'_1 aunque representan el mismo objeto O_1 en el presente ejemplo, no serán estrictamente idénticas. En efecto, ciertos parámetros de captura pueden variar entre las dos imágenes, como el enmarcado, el posicionamiento del objeto, el punto de vista, la escala de representación, el nivel de ruido, la iluminación y/u otro. Tales variaciones son tenidas en cuenta por el algoritmo de tratamiento de las imágenes.

La transmisión 7 de la imagen I'_1 del dispositivo electrónico 2 al servidor 3 puede hacerse por ejemplo en las mismas condiciones que para la imagen I_1, especialmente en términos de formato, de protocolo de transmisión, de modo de aseguramiento (pudiendo ser protegida esta transmisión 7 de la imagen I'_1) y/u otro.

Después de haber recibido la imagen I'_1, el servidor 3 la compara al menos con la imagen I_1 y eventualmente con otras imágenes recibidas durante los registros previos de diversos individuos (etapa 8). A título de ejemplo, si el individuo 1 es objeto de un procedimiento de autenticación, el servidor 3 es capaz de encontrar la imagen I_1 recibida relativa al individuo 1 durante su registro, por ejemplo con la ayuda de una identidad rehusada por el individuo 1. Puede realizarse entonces una comparación entre las dos solas imágenes I_1 e I'_1, con miras a sacar una conclusión sobre el hecho de que el individuo 1 corresponda o no al individuo registrado que éste pretende ser. De acuerdo con otro ejemplo, si el individuo 1 es objeto de un procedimiento de identificación, el servidor 3 puede comparar la imagen I'_1 con todas o parte de las imágenes I_1, $I_{2....}$, I_n recibidas durante los registros previos de diversos individuos, especialmente la imagen I_1 relativa al individuo 1, con miras a sacar una conclusión sobre el hecho de que el individuo 1 corresponda o no a un individuo registrado.

La comparación mencionada anteriormente entre dos imágenes, por ejemplo entre las imágenes I_1 e I'_1, consiste en verificar si las dos imágenes representan o no los mismos objetos, por ejemplo I_1.

Para hacer esto, se puede utilizar cualquier algoritmo conocido y apropiado de comparación de imágenes.

A título de ejemplo no limitativo, se puede utilizar un algoritmo que prevea la búsqueda en cada imagen de descriptores locales, como puntos característicos, informaciones de textura, informaciones de color y/u otros, y después la búsqueda de similitudes entre los descriptores locales de dos imágenes que hay que comparar (graph matching).

Cuando se utilizan puntos característicos de las imágenes como descriptores locales, por ejemplo según la técnica SIFT, SURF o puntos de Harris, se puede ventajosamente buscarles de manera que estos sean invariantes o al menos poco sensibles a un cierto número de transformadores de imagen, como traslaciones, rotaciones, otras transformaciones geométricas, diferencias de iluminación, cambios de escala, cambios de punto de vista, variaciones del nivel de ruido y/u otros. La comparación entre los puntos característicos de dos imágenes puede ser relativamente rudimentaria o bien más sofisticada, por ejemplo utilizando transformadas de Hough, búsquedas por vecindad, y/u otras.

Ejemplos no limitativos de tal algoritmo pueden ser encontrados en los artículos siguientes: « Distinctive Image Features from Scale-Invariant Keypoints » de D. Lowe de fecha 5 de enero de 2004 (a la vista de una publicación en el “Internacional Journal of Computer Vision” en 2004) y « Scale & Affine Invariant Interest Point Detectors » de K. Mikolajczyk y C. Schmid, Internacional Journal of Computer Vision 60(1), 63-86, 2004.

En variante o como complemento, el algoritmo de comparación de imágenes puesto en práctica puede basarse en una detección de contorno de objeto representado por cada imagen, y una comparación de los contornos detectados a partir de su forma (shape matching).

Un ejemplo no limitativo de tal algoritmo puede encontrarse en el artículo siguiente: « Shape Matching and Recognition – Using Generative Models and Informative Features » de Z. Tu y A. Yull de 2004.

Cualquier otro algoritmo de comparación apropiado de imágenes puede ser puesto en práctica con fines de autenticación o de identificación. El sitio http://www.google.com/mobile/goggles/#book por ejemplo da un ejemplo interesante de medios conocidos de puesta en práctica para el reconocimiento de objetos a partir de fotografías tomadas con un teléfono.

Varios algoritmos pueden ser además yuxtapuestos o combinados para mejorar la fiabilidad de la comparación.

Una conclusión C_1 de autenticación o de identificación puede sacarse por el servidor 3 para el individuo 1 teniendo en cuenta el resultado de la comparación de imágenes (etapa 9).

En el marco de un procedimiento de autenticación, si la comparación 8 entre las imágenes I_1 e I'_1 revela una concordancia entre sus respectivos objetos, se puede concluir por ejemplo que el individuo 1 es el individuo registrado que éste pretende ser. En el marco de un procedimiento de identificación, si la comparación 8 entre las imágenes I_1 e I'_1 revela una concordancia entre sus respectivos objetos, se puede concluir por ejemplo que el individuo 1 corresponde a un individuo registrado.

Si, como se describió anteriormente, el servidor 3 ha recibido del dispositivo electrónico 2 un dato personal del individuo 1, por ejemplo una contraseña m_1, como complemento a la imagen I_1 durante la fase de registro del individuo 1, éste puede recibir ventajosamente durante la fase de autenticación o de la identificación, un dato personal correspondiente, por ejemplo una contraseña m'_1 como complemento de la imagen I'_1. En este caso, la conclusión C_1 de autenticación o de identificación sacada por el servidor 3 para el individuo 1 puede resultar no solamente de la comparación de las dos imágenes I_1 e I'_1, sino también de la comparación de los dos datos personales, por ejemplo de las dos contraseñas m_1 y m'_1.

La articulación entre las dos comparaciones puede ser diversa. Por ejemplo, estas dos comparaciones pueden ser efectuadas cada una de manera equivalente. En variante, en el marco de una identificación por ejemplo, el servidor 3 puede empezar por recorrer todos o parte de los datos personales m_1, m_2,…, m_n almacenados para compararlos con los datos personales m'_1. Una vez establecida una selección de los candidatos sobre la base de esta primera comparación de datos personales, el servidor 3 puede entonces comparar la imagen I'_1 con las imágenes almacenadas por o para el servidor 3 relativas a los solos candidatos seleccionados. Se reduce así la cantidad de cálculo necesaria, limitando el número de comparaciones de imágenes puestas en práctica. Pueden considerarse otras articulaciones entre los dos tipos de comparaciones, en variante o como complemento de las que acaban de describirse, como será evidente para el especialista en la materia.

Se observará que, aunque la descripción anterior haya sido descrita con la hipótesis de que una sola imagen I_1 es capturada durante la fase de registro, y comparada con otra imagen durante la fase de autenticación o de identificación, la invención se aplica igualmente al caso en que fueran capturadas varias imágenes I_1 ligadas o no, durante la fase de autenticación o de identificación. Se incrementa así la discriminación y, por tanto, la fiabilidad de la autenticación o de la identificación.

Como se mencionó anteriormente, el servidor 3 utilizado podría diferir de un único servidor. A título de ejemplo, éste podría estar compuesto de varias entidades que aseguren funciones respectivas.

Un ejemplo no limitativo de tal sistema de verificación distribuido podría quedar dispuesta como sigue: una primera entidad del sistema de verificación podría recibir las imágenes I_1 e I'_1 y eventualmente asegurar su comparación, mientras que una segunda entidad del sistema de verificación se encargaría de al menos una parte de la verificación propiamente dicha, eventualmente en cooperación con la primera entidad. En tal escenario, la primera entidad podría comprender por ejemplo una tarjeta inteligente y/o un terminal eventualmente colocalizado con (o embarcado en) al menos uno de los dispositivos electrónicos utilizados por el individuo 1 considerado, o situado en la proximidad de éste, mientras que la segunda entidad podría consistir por ejemplo en un servidor simple, por ejemplo desprovisto de módulo de tratamiento de imagen.

En este escenario, en caso de concordancia entre los objetos de las imágenes I_1 e I'_1, la primera entidad podría por ejemplo generar una clave a partir de la imagen I_1 y/o de la imagen I'_1, después esta clave podría ser utilizada durante un diálogo protegido entre la primer entidad y la segunda entidad con fines de verificación, es decir para autenticar y/o identificar al individuo 1 considerado. La clave en cuestión podría comprender por ejemplo un valor numérico correspondiente a la imagen I_1 y/o la imagen I'_1, eventualmente después de la aplicación de una función criptográfica, como por ejemplo una función de comprobación aleatoria. La verificación podría consistir entonces por ejemplo en una transmisión protegida de la clave de la primera entidad a la segunda entidad, y después en una comparación por la segunda entidad de la clave así recibida con una clave obtenida previamente relativa al individuo 1.

Naturalmente, pueden considerarse igualmente otros mecanismos y otras arquitecturas relativas al sistema de verificación, como será evidente para el especialista en la materia.

Todas o parte de las operaciones que han sido descritas hasta ahora pueden ser puestas en práctica por uno o varios programas de ordenador que comprenda instrucciones de código apropiadas. A título de ejemplo, un programa de ordenador puede estar cargado y ser ejecutado en un dispositivo electrónico y/o a nivel del sistema de verificación para poner en práctica las operaciones respectivamente a cargo de estas diferentes entidades.

REIVINDICACIONES

1. Procedimiento para permitir la autenticación o la identificación de un individuo (1) con la ayuda de un primer dispositivo electrónico (2) que comprende una unidad de captura de imagen y una unidad de transmisión de datos, incluyendo el procedimiento una fase de registro del citado individuo en un sistema de verificación (3), comprendiendo la fase de registro las etapas siguientes:

- captura de una primera imagen (I_1) de al menos un objeto (O_1) cualquiera elegido secretamente por el individuo, con la ayuda de la unidad de captura de imagen del citado primer dispositivo electrónico;
- transmisión, con la ayuda de la unidad de transmisión de datos del citado primer dispositivo electrónico, de la citada primera imagen al sistema de verificación;

incluyendo el procedimiento además una fase de autenticación o de identificación relativas al citado individuo (1) con la ayuda de un segundo dispositivo electrónico (2), comprendiendo la fase de autenticación o de identificación las etapas siguientes puestas en práctica a nivel del sistema de verificación (3):

- recepción desde el segundo dispositivo electrónico de una segunda imagen (I'_1) de al menos un objeto (O_1) idéntico o similar al de la primera imagen (I_1);
- comparación de la segunda imagen al menos con la primera imagen;
- conclusión de que el individuo está autenticado o identificado con éxito cuando la comparación de la segunda imagen con la primera imagen revela una concordancia entre sus respectivos objetos;

en el cual la segunda imagen es una imagen no registrada ni adquirida previamente para las necesidades de la comparación en el momento de la autenticación o de la identificación del individuo.

2. Procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual el objeto (O_1) elegido por el individuo (1) es un objeto que el individuo lleva siempre consigo o está a su alcance.

3. Procedimiento de acuerdo con las reivindicaciones 1 o 2, en el cual la primera imagen (I_1) es transmitida al sistema de verificación (3) de modo protegido.

4. Procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual al menos un primer dato personal (m_1) del citado individuo (1) es transmitido al sistema de verificación (3) como complemento de la primera imagen (I_1).

5. Procedimiento de acuerdo con la reivindicación 4, que comprende además la recepción desde el segundo dispositivo electrónico (2) de un segundo dato personal del citado individuo (1) correspondiente al primer dato personal (m_1) y la comparación del segundo dato personal al menos con el primer dato personal, y en el cual se concluye que el individuo es autenticado o identificado con éxito cuando la comparación de la segunda imagen (I'_1) con la primera imagen (I_1) revela una concordancia entre sus respectivos objetos y la comparación del segundo dato personal con el primer dato personal revela una concordancia entre el segundo dato personal y el primer dato personal.

6. Procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual el primer dispositivo electrónico (2) y/o el segundo dispositivo electrónico (2) son un mismo dispositivo.

7. Procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual el primer dispositivo electrónico (2) y/o el segundo dispositivo electrónico (2) pertenecen al citado individuo (1).

8. Procedimiento de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual la segunda imagen (I'_1) es transmitida al sistema de verificación (3) desde el segundo dispositivo electrónico (2) de modo protegido.

9. Sistema de verificación (3) para permitir la autenticación o la identificación de un individuo (1) de acuerdo con una cualquiera de las reivindicaciones precedentes, comprendiendo el sistema de verificación:

- una primera unidad de recepción para recibir, desde un primer dispositivo (2), una primera imagen (I_1) capturada de al menos un objeto (O_1) cualquiera elegido secretamente por el individuo;
- una segunda unidad de recepción para recibir, desde un segundo dispositivo electrónico (2), una segunda imagen (I'1) de al menos un objeto (O1) idéntico o similar al de la primera imagen;
- un comparador de imágenes para comparar la segunda imagen con al menos la primera imagen;
- una unidad de decisión para concluir que el individuo es autenticado o identificado con éxito cuando la comparación de la segunda imagen con la primera imagen efectuada por el comparador revela una concordancia entre sus respectivos objetos;

en el cual la segunda imagen es una imagen no registrada ni adquirida previamente para las necesidades de la comparación en el momento de la autenticación o de la identificación del individuo.

10. Sistema de verificación de acuerdo con la reivindicación 9, estando distribuido el citado sistema de verificación entre varias entidades.

11. Producto programa de ordenador que comprende las instrucciones de código para poner en práctica el procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 8, cuando éste está cargado y es ejecutado en medios informáticos.

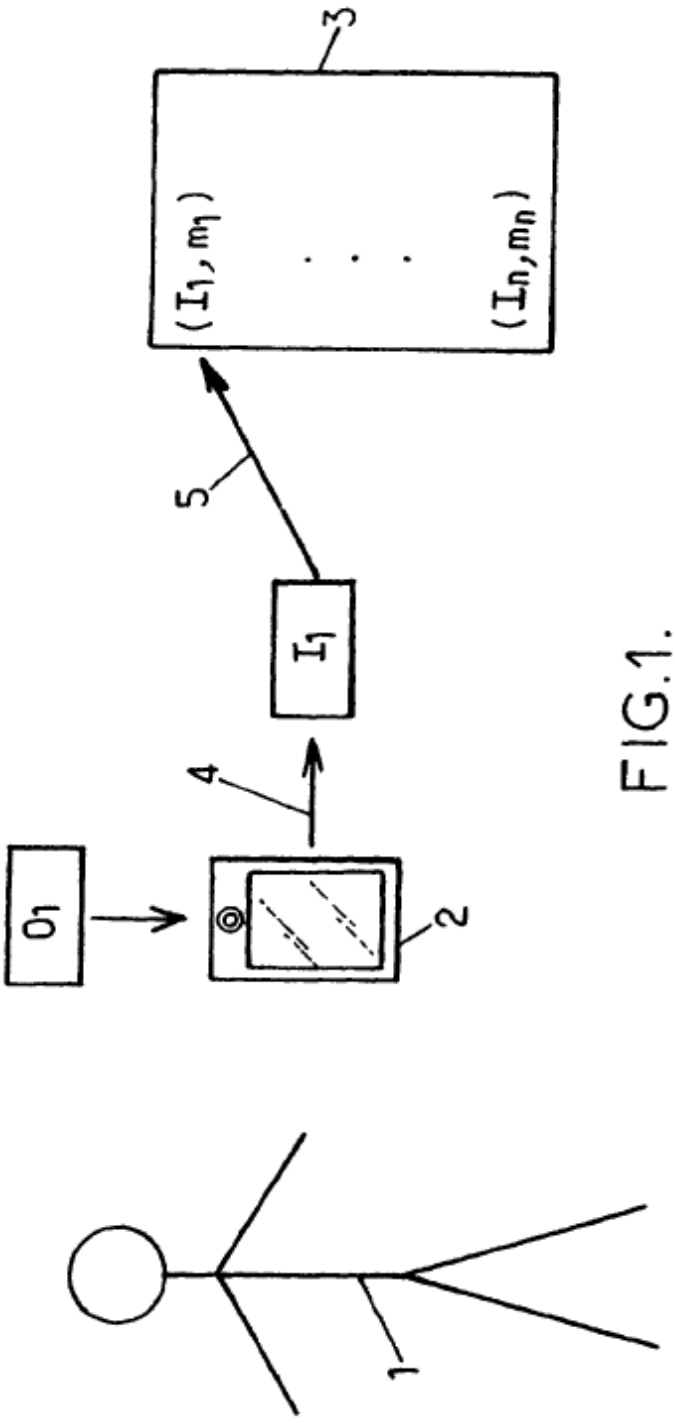

FIG.1.

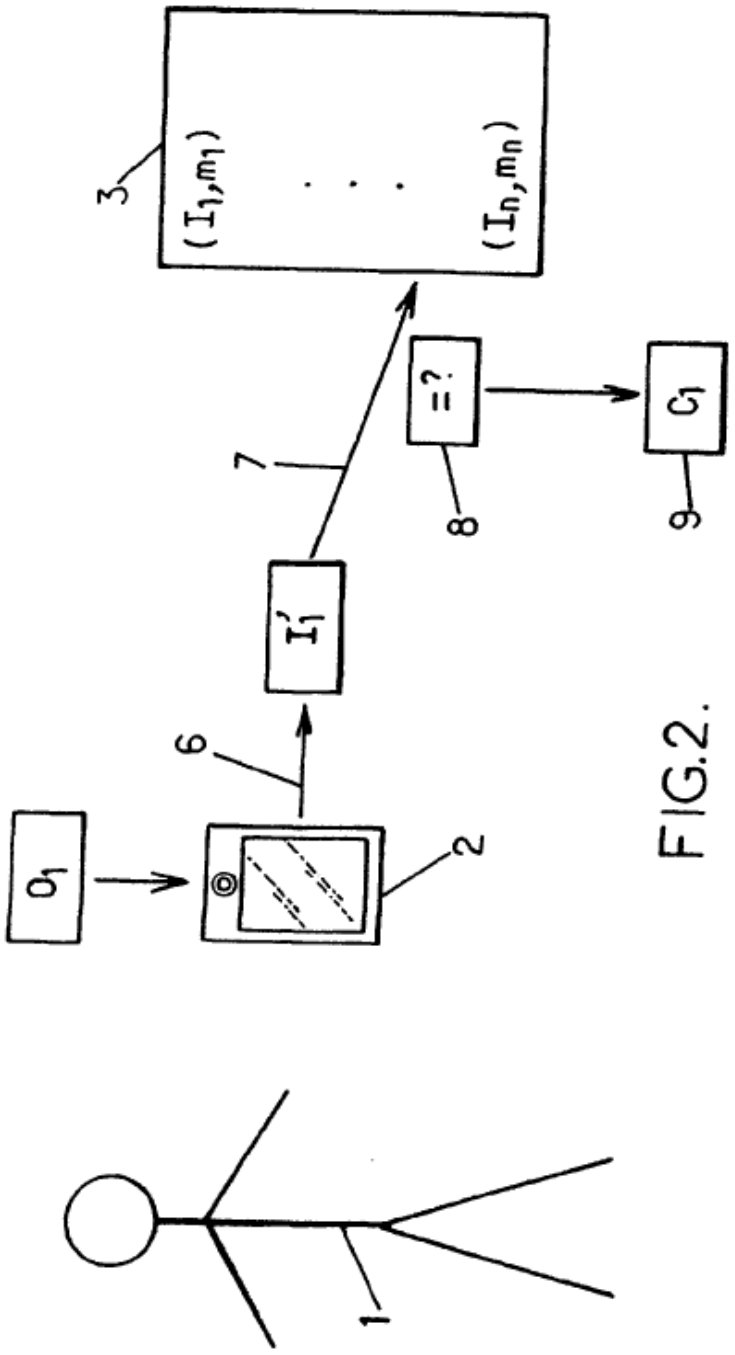

FIG.2.