(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 295 117**

(51) Int. Cl.:
G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01400338 .8**
(86) Fecha de presentación : **09.02.2001**
(87) Número de publicación de la solicitud: **1126419**
(87) Fecha de publicación de la solicitud: **22.08.2001**

(54) Título: **Procedimiento y dispositivo de autentificación con seguridad de una persona, mediante detección de una característica biométrica, para una autorización de acceso.**

(30) Prioridad: **15.02.2000 FR 00 01848**

(45) Fecha de publicación de la mención BOPI:
16.04.2008

(45) Fecha de la publicación del folleto de la patente:
16.04.2008

(73) Titular/es: **SAGEM Sécurité**
Le Ponant de Paris 27, rue Leblanc
75015 Paris, FR

(72) Inventor/es: **Chabanne, Hervé Patrick Julien**

(74) Agente: **Carpintero López, Francisco**

DESCRIPCIÓN

Procedimiento y dispositivo de autentificación con seguridad de una persona, mediante detección de una característica biométrica, para una autorización de acceso.

La presente invención se refiere a perfeccionamientos aportados en el ámbito de la seguridad de la memorización y/o transferencia de información representativa de la imagen detectada de por lo menos una característica biométrica de una persona con objeto de una autentificación seguridad de la persona para autorizar a ésta a un acceso, especialmente por medio de un código de identificación personal (conocido en la técnica con el nombre de código PIN).

En el resto de la descripción, se pretende proporcionar al término "acceso" un sentido general, es decir tanto el sentido de acceso físico, por ejemplo mediante la apertura de una puerta o equivalente, a un local o edificio bajo control, como el sentido de acceso a un servicio a través de un dispositivo adecuado (por ejemplo, acceso a un sistema bancario, utilización de un teléfono, especialmente un teléfono móvil, utilización de un ordenador, etc.).

Hasta la fecha, la autorización de acceso suele basarse en el uso de un código PIN que posee el usuario y que puede ser empleado junto con una tarjeta con chip. En el caso cada vez más frecuente en que el usuario debe tener acceso a varios servicios y/o aparatos, es necesario que memorice varios códigos PIN, lo que puede generar problemas (olvido, confusión, inversión, etc.).

Además, la confidencialidad de memorización del código PIN en el aparato o tarjeta utilizada no está siempre asegurada: por ello, se memoriza el código PIN sin codificar en la memoria del chip microelectrónico contenido en las tarjetas bancarias.

Se conoce asimismo el hecho de sustituir y/o completar el código PIN por otra información característica del usuario. Así es como se conoce el hecho de recurrir a tal efecto a una característica física, o característica biométrica, del usuario (huellas dactilares de uno o varios dedos, geometría de una o ambas manos, iris y/o retina de uno o ambos ojos, geometría del rostro, etc.) y completar y/o sustituir el código PIN por la detección de por lo menos una característica biométrica.

El documento FR 2 671 210 se refiere a un procedimiento de identificación y autentificación de datos que caracterizan a un individuo mediante comprobación de dichos datos por medio de un biómetro, procedimiento según el cual se procede a un tratamiento idéntico de la huella del individuo previamente registrada y mantenida en memoria en una tarjeta de memoria y de su huella recogida en el biómetro, el cual tratamiento consiste en organizar virtualmente grupos secuenciales de palabras en sub-bloques matriciales, en organizar virtualmente los sub-bloques matriciales en un único bloque matricial, en realizar permutas de palabras en el interior de los sub-bloques matriciales, en determinar una palabra de paridad para cada línea del bloque matricial, en comparar las palabras de paridad obtenidas en la tarjeta y el biómetro, y en tratar la huella en función del resultado de dicha comparación.

En cualquier caso, el problema que se plantea reside en la seguridad de la memorización y/o de la transferencia de los datos de identificación de la persona, con objeto de evitar que dichos datos puedan ser detectados por un tercero que tuviera acceso a la memoria y/o que pudiera conectarse a la línea de transmisión de los datos, y que, a continuación, pudiera utilizar o hacer utilizar dichos datos de forma fraudulenta.

Por lo tanto, la invención tiene esencialmente por objeto proponer medios particulares orientados a proporcionar seguridad en la memorización/transferencia de datos de identificación de una persona, con objeto de una autorización de acceso de la misma, especialmente por medio de un código PIN.

Con tal fin, la invención propone un procedimiento de autentificación con seguridad de una persona, para autorizar a ésta a un acceso, mediante la detección de características biométricas de dicha persona, el cual procedimiento se caracteriza, estando constituido de conformidad con la invención, porque incluye las etapas indicadas en la reivindicación 1.

De este modo, se constituye una imagen codificada de dichas características biométricas, que está constituida por un grupo de n subconjuntos transformados que representa una combinación de transformaciones entre todas las combinaciones de posibles transformaciones en los n subconjuntos de características.

De manera preferente, el grupo de n subconjuntos de características es transformado, por lo menos una primera vez, y dicha primera transformación consiste en una traslación-permuta aplicada a por lo menos una pareja de subconjuntos de características: en este caso, la operación de traslación-permuta de los subconjuntos de características biométricas constituye la transformación fundamental que se utiliza sistemáticamente. Esta transformación puede ser selectiva, es decir aplicarse sólo a una única pareja de subconjuntos, o aplicarse a varias parejas de subconjuntos, o aplicarse a todos los subconjuntos.

En la práctica, esta única etapa de transformación ofrece un número de combinaciones suficientemente elevado como para conducir a una seguridad aceptable de la codificación de la imagen detectada de las características biométricas de la persona, y se puede plantear perfectamente limitar la transformación de los subconjuntos de características biométricas a esta única etapa de traslación-permuta.

Si se desea incrementar la seguridad aumentando el número de posibles combinaciones, se puede recurrir a una segunda transformación, que se efectúa en el grupo de los subconjuntos de características resultante de la primera transformación, y la segunda transformación consiste en una rotación, respectivamente una homotecia, efectuada en por lo menos un subconjunto o en cada uno de por lo menos ciertos subconjuntos de dicho grupo resultante de la primera transformación.

Se puede incrementar asimismo el número de posibles combinaciones de las transformaciones recurriendo a una tercera transformación que se efectúa en el grupo de subconjuntos de características resultante de la segunda transformación y la tercera transformación consiste en una homotecia, respectivamente una rotación, efectuada en por lo menos un subconjunto o en cada uno de por lo menos algunos subconjuntos de dicho grupo resultante de la segunda transformación.

También en este caso, tanto la segunda transformación como la tercera transformación pueden afectar a todo o parte de los subconjuntos. Además, el sentido y el ángulo de la rotación y la relación de la homotecia pueden variar de un subconjunto a otro, lo que complica aún más una detección inversa fraudulenta.

Además, se puede añadir en el grupo de los subconjuntos de características, antes de la primera transformación y/o entre dos transformaciones y/o tras la última transformación, por lo menos un falso subconjunto de características (señuelo). Gracias a esta adición de señuelos, se incrementa el número de subconjuntos del conjunto codificado conseguido a fin de cuentas y, por lo tanto, se aumenta el número de combinaciones de posibles transformaciones, lo que incrementa la seguridad: un tercero que detectase los subconjuntos codificados de características biométricas debería, para intentar descubrir el conjunto de origen, probar todas las posibles combinaciones, las cuales, incluso con un número relativamente restringido de subconjuntos (por ejemplo media docena) y un pequeño número de etapas de transformación (por ejemplo de una a tres), están en número considerable, lo que imposibilita el intento en la práctica con la ayuda de medios habituales.

Cabe subrayar aquí que el conjunto y los subconjuntos de características biométricas no están constituidos por la imagen misma (imagen fotográfica) de la característica biométrica detectada en la persona (por ejemplo la huella digital de uno de sus dedos), sino por datos digitales que definen los puntos o puntos singulares de dicha característica biométrica.

En estas condiciones, las transformaciones indicadas anteriormente no son todas de misma naturaleza:

- en la traslación-permuta, existe desplazamiento físico del subconjunto que, desde un emplazamiento inicial en el resto de subconjuntos, consigue llegar a otro emplazamiento en el resto; en el transcurso de dicha transformación se modifican las coordenadas de los puntos anotados;

- por el contrario, en la rotación y la homotecia, el subconjunto transformado conserva su emplazamiento en el resto; pero los datos de este subconjunto se modifican (cambian y/o completan) para integrar la nueva posición angular (sentido y amplitud) o la nueva escala (relación de homotecia) de los puntos característicos definidos por dicho subconjunto.

Gracias al procedimiento de codificación que se acaba de describir, es posible memorizar y/o transmitir de forma seguridad el conjunto codificado de las características biométricas de la persona; la restitución del conjunto de origen se efectúa empleando algoritmos de reconocimiento biométrico conocidos, insensibles a las transformaciones, como se expone a continuación.

En un modo de puesta en práctica del procedimiento de la invención:

- se empieza por constituir el conjunto no codificado de características biométricas que se graba en una memoria protegida,

- en cada solicitud de acceso de la persona, se establece el grupo de subconjuntos codificados de características biométricas y se transmite dicho grupo de subconjuntos codificados a la memoria, para comparación de éste con el conjunto no codificado de características conservado en memoria,

- en función del resultado de la comparación, se emite una instrucción hacia la solicitud de acceso para autorizar o prohibir el acceso de la persona.

En otro modo de puesta en práctica de dicho procedimiento de autentificación con seguridad según la invención:

- se empieza por detectar las características biométricas de la persona y por constituir el grupo de subconjuntos codificados de características biométricas que se graba en una memoria,

- en cada solicitud de acceso de la persona, se detectan las características biométricas de la persona y se constituye el conjunto no codificado de sus características biométricas,

- se extrae de la memoria el grupo de subconjuntos codificados de características que se transmite hacia la solicitud de acceso, donde es comparado con el conjunto no codificado, y

- en función del resultado de la comparación, se emite una instrucción para autorizar o prohibir el acceso de la persona.

En uno y otro modo de puesta en práctica anteriores, el conjunto no codificado no está ni memorizado en una memoria no protegida, ni transmitido a distancia, de manera que un tercero sólo puede tener acceso a los subconjuntos codificados cuyo uso le está prohibido en la práctica dado el número demasiado elevado de combinaciones a probar.

Para aclarar las ideas, si el conjunto inicial de características biométricas se divide en seis subconjuntos, si se añaden doce falsos subconjuntos o señuelos, y si el número de transformaciones es de diez, el número de posibles combinaciones es

$$C^{18}_{6} \times 10^{6} = 18564000000.$$

En la práctica, se limita este número de combinaciones, limitando el número de posibles transformaciones o utilizando códigos correctores de errores para incrementar la fiabilidad del sistema.

Por ejemplo, se limita a tres el número de transformaciones (permuta, rotación, homotecia); sin embargo, el número de posibles combinaciones sigue siendo de

$$C^{18}_{6} \times 3^{6} = 13153156.$$

En estas condiciones, la detección fraudulenta de los subconjuntos codificados no puede llevarse a cabo de forma práctica para conducir a una reconstitución de la imagen completa de origen.

En la práctica, la comparación de los subconjuntos codificados y el conjunto no codificado se realiza comparando sucesivamente los subconjuntos codificados de características, a través de los algoritmos insensibles a las transformaciones, con el conjunto no codificado de características biométricas hasta las coincidencias respectivas de los subconjuntos codificados con partes respectivas del conjunto no codificado. Dicha comparación representa una tarea no demasiado compleja, que puede llevar a cabo el terminal ante el que la persona se presenta para conseguir su autorización de acceso.

Con preferencia, en caso de no coincidencia de un subconjunto codificado de características con una parte del conjunto de características no codificado, se hace intervenir un código corrector de error y se emite una autorización de acceso si una proporción determinada de los n subconjuntos codificados encuentra, tras una corrección de error eventual, correspondencias respectivas en el conjunto no codificado, mientras que se emite una prohibición de acceso si dicha proporción predeterminada de subconjuntos codificados, tras la corrección de error eventual, no encuentra correspondencias respectivas en el conjunto no codificado.

Para fiabilizar la autentificación de la persona, se puede prever además que, tras la puesta en correspondencia de los subconjuntos codificados con el conjunto no codificado, se compare el grupo de los subconjuntos codificados y el conjunto no codificado desde el punto de vista de por lo menos una característica adicional no detectable en los subconjuntos codificados individuales y no tenidos en cuenta en las etapas anteriores y sólo emite una autorización de acceso en caso de correspondencia mayoritaria también en dicha característica adicional.

En un gran número de aplicaciones previstas por la invención, las características biométricas son las de las huellas dactilares de por lo menos un dedo de la persona.

En este caso, para incrementar la precisión del sistema, se puede prever que las características biométricas sean las de las huellas dactilares de varios dedos de la persona. Para no aumentar de forma desproporcionada el número de subconjuntos a tratar, se puede prever que, siendo p el número de dedos utilizado, se establezca para cada dedo un número n/p de subconjuntos de características biométricas, con objeto de que el número total de subconjuntos de características sea igual a n.

Para añadir aún más información, se puede prever asimismo que, pudiendo clasificarse las huellas dactilares de los dedos de las manos en k tipos generales, se determine, durante la detección de las características de las huellas dactilares de la persona, el tipo K al que pertenecen, utilizándose el tipo K como información adicional de los subconjuntos codificados.

Una aplicación especialmente interesante del procedimiento que se acaba de describir reside en la autentificación seguridad de una persona titular de un código de identificación o código PIN. En efecto, en dicho caso, el procedimiento puede consistir, de conformidad con la invención, en que:

- se pone en práctica el procedimiento de autentificación seguridad que se acaba de describir;

- en el transcurso de la comparación de los subconjuntos codificados con el conjunto no codificado a través de los algoritmos insensibles a las transformaciones, se detecta, por medio de dichos algoritmos, la combinación de las transformaciones experimentadas anteriormente por los subconjuntos codificados,

- se elabora, especialmente a partir de la combinación de las transformaciones detectadas por los algoritmos insensibles a las transformaciones, una clave que se considera como código PIN asignado a la persona, y

- finalmente, se utiliza el código PIN así elaborado para comandar la autorización de acceso de la persona.

Dicho procedimiento de generación automática del código PIN que proporciona la autorización de acceso a la persona es especialmente interesante, ya que no sólo libera a la persona de tener que memorizar continuamente su código PIN, sino que también permite securizar todo el proceso de autorización de acceso.

Además, el código PIN se genera automática e independientemente de la persona: por lo tanto, se puede evitar el código alfanumérico tradicionalmente utilizado y hacer que el código PIN sea una función cualquiera tan compleja como se desee.

A título de ejemplo, se puede prever la generación de una clave intermedia formada por la combinación C(i, t), donde i es el índice de cada subconjunto correspondiente a la transformación que le ha sido aplicada, y t la transformación que le ha sido aplicada. Se puede establecer entonces una clave final, teniendo en cuenta que una cantidad de información más importante, que resulta, por ejemplo en el caso en que la característica biométrica está constituida por las huellas dactilares de por lo menos un dedo de la persona, de la concatenación de dicha clave intermedia y otra información, por ejemplo la ligada a la clasificación (tipo) de la huella, la frecuencia de los surcos, u otros datos relativos a las minucias (puntos característicos de las huellas) tales como la valencia (bifurcación o fin de los surcos) o la curvatura general de los surcos alrededor del punto característico. Se añade entonces un código de error que conduce a un código final capaz de hacer oficio de código PIN.

Siguiendo con el mismo objetivo, se puede plantear asimismo que el procedimiento pueda consistir, de conformidad con la invención, en que:

- se pone en práctica el procedimiento de autentificación con seguridad descrito anteriormente,

- en el transcurso de la comparación de los subconjuntos codificados con el conjunto no codificado a través de los algoritmos insensibles a las transformaciones, se detecta, mediante dichos algoritmos, la combinación de las transformaciones experimentadas anteriormente por los subconjuntos codificados,

- se busca la combinación así encontrada de las transformaciones en una tabla que encierra, por una parte, una lista de combinaciones de posibles transformaciones y, por otra parte, una lista de códigos PIN que están en relación biunívoca, y se anota el código PIN en relación con la combinación encontrada, y

- finalmente, se utiliza el código PIN seleccionado para comandar la autorización de acceso de la persona.

En este caso, es posible que la persona conozca su código PIN, que puede ser una simple palabra alfanumérica, y la puesta en práctica del procedimiento de la invención permite la búsqueda seguridad y la emisión automática de dicho código PIN a partir de la simple lectura de una característica biométrica de la persona.

Además, puede ser ventajoso prever que en caso de una puesta en práctica no válida de uno u otro procedimiento que se acaba de indicar (disfunción de los aparatos, mala lectura de la característica biométrica, etc.), la persona esté autorizada a introducir manualmente, por medio de un teclado, un código PIN que posee personalmente, que puede ser bien el mismo que el generable automáticamente, o distinto.

En este caso, se trata de una combinación de ambos sistemas, es decir la asociación a cada persona de dos códigos PIN, uno complejo emitido automáticamente, que queda ignorado por la persona y otro conocido por la persona y utilizado manualmente sólo cuando la persona está autorizada.

Según otro de sus aspectos, la invención propone asimismo un dispositivo de autentificación con seguridad de una persona para autorizar a ésta a un acceso, mediante detección de por lo menos una característica biométrica de dicha persona, para la puesta en práctica del procedimiento de autentificación descrito anteriormente, el cual dispositivo, estando dispuesto de conformidad con la invención, se caracteriza como se indica en la reivindicación 18.

Con preferencia, dichos medios transformadores algorítmicos son capaces de efectuar por lo menos una primera transformación del tipo traslación-permuta, y eventualmente una segunda y tercera transformación del tipo rotación, respectivamente homotecia. Además, ventajosamente, el dispositivo puede incluir medios generadores de falsos subconjuntos capaces de generar por lo menos un falso subconjunto e introducirlo como señuelo entre los subconjuntos de características biométricas, lo que incrementa el número de subconjuntos en el conjunto codificado.

Además, dicho dispositivo de autentificación con seguridad puede tener una aplicación especialmente interesante para la puesta en práctica del procedimiento descrito anteriormente cuando la persona es titular de un código PIN que

la autoriza a un acceso, un modo de realización de dicho dispositivo estando dispuesto de conformidad con la invención, caracterizándose porque los medios generadores de una instrucción de autorización son capaces, a partir de las transformaciones que los algoritmos insensibles a las transformaciones han detectado en los subconjuntos codificados, de determinar la combinación correspondiente de las transformaciones y de elaborar, a partir de dicha combinación, una clave utilizable como código PIN.

Otro modo de realización de dicho dispositivo realizado de conformidad con la invención se caracteriza porque:

- incluye segundos medios de memorización que encierran una tabla de relaciones biunívocas entre una multiplicidad de combinaciones entre las que figura la combinación particular de las transformaciones experimentadas por los subconjuntos codificados, y una multiplicidad equivalente de códigos PIN entre los que figura, en correspondencia con dicha combinación particular, el código PIN asignado a la persona,

- los algoritmos incluidos en los medios de comparación son capaces de detectar las transformaciones experimentadas por los subconjuntos codificados, y de detectar la combinación de dichas transformaciones,

- incluye segundos medios comparadores capaces de comparar la combinación de las transformaciones restituida por los algoritmos y las combinaciones contenidas en la tabla de segundos medios de memorización, y

- los medios generadores de una instrucción de autorización están situados bajo la dependencia de dichos segundos medios comparadores y son capaces de generar el código PIN correspondiente a la combinación detectada con destino a un órgano de autorización de acceso comandado por dicho PIN.

Es entonces posible hacer que el dispositivo incluya, además, medios de introducción manual del o de un código PIN por parte de la persona y que los medios de introducción manual estén situados bajo la dependencia de dichos medios generadores, para ser inhibidos cuando el dispositivo es capaz de generar automáticamente la búsqueda y la emisión del código PIN y para ser activados cuando no es posible la generación automática del código PIN.

En un modo de realización capaz de convenir para numerosas aplicaciones, los medios sensores son capaces de detectar las huellas dactilares de por lo menos un dedo de la persona.

La invención se entenderá mejor mediante la lectura de la siguiente descripción de algunos modos de realización preferidos, proporcionados únicamente a título de ejemplos no limitativos. En dicha descripción, se hace referencia a los dibujos adjuntos, en los cuales:

- las figuras 1A, 1B y 2 a 6 ilustran diversas etapas del procedimiento de codificación de una imagen detectada de características biométricas de una persona, de conformidad con la invención;

- la figura 7 muestra un esquema sinóptico que ilustra un modo de realización de un dispositivo conforme a la invención, para la puesta en práctica del procedimiento de codificación de una imagen detectada de características biométricas de una persona;

- las figuras 8 y 9 muestran dos esquemas sinópticos que ilustran respectivamente dos modos de realización de un dispositivo de autentificación con seguridad de una persona, para autorizar a ésta a un acceso, de conformidad con la invención; y

- las figuras 10 y 11 muestran dos esquemas sinópticos que ilustran respectivamente dos modos de realización de un dispositivo de autentificación con seguridad de una persona titular de un código de autentificación personal PIN que la autoriza a un acceso, de conformidad con la invención.

En la siguiente descripción, se hace referencia más concretamente a la característica biométrica constituida por las huellas dactilares de uno varios dedos de por lo menos una mano de una persona, ya que se trata de un caso destinado a un gran desarrollo, quedando entendido, sin embargo, que la puesta en práctica de la invención puede llevarse a cabo sobre la base de cualquier otra característica biométrica de la persona, incluso sobre la base de una combinación de varias características biométricas de misma naturaleza (huellas dactilares de varios dedos, por ejemplo) o de distinta naturaleza (huella dactilar de un dedo e iris de un ojo, por ejemplo).

Con la ayuda de un sensor adecuado conocido por el especialista en la materia, se detecta por lo menos una característica biométrica de la persona, en este caso estando constituida dicha característica biométrica por la huella dactilar 1 de uno de sus dedos (figura 1A que muestra la huella 1 a escala ampliada). Se establece así un conjunto 2 de características biométricas (o "template") que caracterizan la huella 1 (por ejemplo las minucias), y se divide el conjunto 1, como se ilustra en la figura 1B, en un número n de subconjuntos (o "sub-templates"). En el ejemplo de la figura 1B, los subconjuntos son seis y son designados mediante la referencia alfabética A a F.

Para facilitar la comprensión, se ha superpuesto en la figura 1A la representación de tipo fotográfico de la huella 1 y la esquematización en forma de un rectángulo dividido del conjunto 2 de características biométricas detectadas (que en la práctica está formado por un conjunto de datos que caracterizan los puntos singulares de la huella).

De este modo, del conjunto 2 de características biométricas, se extrae una serie de n subconjuntos A a F (figura 2), quedando entendido que las referencias A a F indicadas en la figura 1B son totalmente arbitrarias y podrían ser distintas si fuese necesario.

Se aplica entonces a por lo menos uno de los subconjuntos o a cada uno de por lo menos algunos subconjuntos por lo menos una transformación geométrica del tipo traslación-permuta y/o rotación y/o homotecia. En la práctica, el orden de las transformaciones, cuando se efectúan varias transformaciones sucesivas, importa poco.

Cada subconjunto puede ser objeto de una transformación con independencia de las demás imágenes, dicho de otro modo, sólo pueden transformarse algunos subconjuntos, y el sentido y amplitud de la transformación (rotación, homotecia) pueden variar de un subconjunto a otro.

Cuando está prevista una única transformación, se puede (pero no es obligatorio) plantear que se trata de una traslación-permuta como se ilustra en la figura 3: a título de ejemplo, los subconjuntos A y C han sido permutados y los subconjuntos E y D han sido permutados, mientras que los subconjuntos B y F no son transformados. En una transformación mediante traslación-permuta, se modifican las coordenadas de los puntos anotados.

En este caso, cuando está prevista una segunda transformación después de la primera, se puede tratar de una rotación o una homotecia. En el ejemplo de la figura 4, se ha supuesto una rotación que afecta a todo o parte de los subconjuntos de la figura 3. A título de ejemplo, el subconjunto C no experimenta rotación alguna, mientras que los demás subconjuntos experimenta cada uno una rotación bien dextrógira (B, E, D), bien levógira (A, F). Además, la amplitud de las rotaciones puede ser bien la misma para todos los subconjuntos con un valor predeterminado conservado para cada operación de codificación, bien ser la misma para todos los subconjuntos con un valor que varíe en cada operación, bien con valores distintos para todos los subconjuntos o algunos subconjuntos.

Cuando se efectúa una tercera transformación en los subconjuntos resultantes de la segunda transformación, se trata de una homotecia, respectivamente de una rotación. En el ejemplo de la figura 5, que viene de la rotación de la figura 4, se trata de una homotecia que afecta a todo o parte de los subconjuntos de la figura 4. En este ejemplo, los subconjuntos B y F no experimentan transformación homotécica, mientras que los demás subconjuntos son transformados con una primera relación (A, E) o con una segunda relación de homotecia (C, D). Por supuesto, se puede plantear una relación de homotecia superior a 1 (ampliación).

Por supuesto, el grupo de los subconjuntos transformados mediante homotecia de la figura 5 puede constituir la segunda etapa de transformación que sigue inmediatamente a la primera etapa (permuta de la figura 3).

En una transformación mediante rotación u homotecia, los datos del subconjunto se modifican (cambian y/o completan) para mostrar los datos capaces de identificar la nueva posición angular o, respectivamente, la nueva escala.

Se puede aumentar además el número de combinaciones artificialmente, para un número n dado de subconjuntos, introduciendo en cualquier etapa (antes, durante o después de las transformaciones), uno o varios falsos subconjuntos o señuelos L como se ilustra en la figura 6 (que corresponde por ejemplo al orden de los subconjuntos resultantes de la permuta como se ilustra en la figura 3).

Para la puesta en práctica del procedimiento que se acaba de describir, se puede recurrir a un dispositivo de codificación de una imagen detectada de características biométricas de una persona, como se ilustra en la figura 7 de los dibujos adjuntos.

Dicho dispositivo incluye medios sensores 3 capaces de detectar una característica biométrica, en este caso la huella dactilar 1 de un dedo de la persona. Unos medios de tratamiento 4, situados bajo la dependencia de los anteriores, son capaces de proporcionar un conjunto 2 de características biométricas (es decir un conjunto de datos que identifican puntos singulares tales como las minucias de la huella 1).

Unos medios de división 5 dividen el conjunto 2 en un número n de subconjuntos de características biométricas, por ejemplo en seis subconjuntos A a F.

Finalmente, los subconjuntos resultantes de la división son tratados por medios transformadores algorítmicos 6 capaces de hacer experimentar eventualmente a cada subconjunto una transformación mediante traslación permuta y/o una rotación y/o una homotecia. Los medios transformadores algorítmicos son aquí supuestamente distintos según el tipo de transformación efectuada y se designan respectivamente mediante P para la traslación-permuta, R para la rotación y H para la homotecia. Pero también puede tratarse de los mismos medios algorítmicos capaces de efectuar una de dichas transformaciones en función de un parámetro de comando.

Los medios transformadores 6 pueden estar dispuestos para efectuar cualquier transformación P, R o H en los subconjuntos, o varias transformaciones sucesivas en un orden cualquiera. Sin embargo, dado que la transformación mediante traslación-permuta P conduce a un número de combinaciones suficientemente elevado para ciertas aplicaciones y es además fácil de poner en práctica, se puede prever que los subconjuntos estén sometidos a por lo menos esta transformación P: por lo tanto, los medios transformadores algorítmicos P se sitúan a la cabeza de los medios 6.

A la salida S de los medios 6, se recoge un grupo de subconjuntos de características biométricas que son codificados mediante las transformaciones P y/o R y/o H, constituyendo dicho grupo de subconjuntos una combinación entre todas las posibles combinaciones.

Para incrementar artificialmente el número de posibles combinaciones para un número n dado de subconjuntos, se puede plantear la incorporación al dispositivo de un generador GL de falsos subconjuntos o señuelos L que sea capaz de introducir dichos señuelos en cualquier lugar deseado, bien aguas arriba, bien aguas debajo de los medios transformadores 6, bien entre los medios transformadores específicos P, R o H.

Gracias al dispositivo de codificación, se obtiene un conjunto codificado de características biométricas que puede utilizarse de forma seguridad, por ejemplo para ser grabado o transmitido.

Una aplicación particular, objeto de la invención, del procedimiento y del dispositivo de codificación que se acaban de describir, afecta a la autentificación seguridad de una persona para autorizar a ésta a un acceso, mediante la detección de características biométricas.

Para ello, con un desfase en el tiempo bien antes, bien después del establecimiento del grupo de dichos subconjuntos codificados, se detectan las características biométricas de la persona y se establece un conjunto no codificado de dichas características biométricas. Se graba el grupo de subconjuntos codificados o el grupo de subconjuntos no codificados que se ha establecido en primer lugar en el tiempo. Durante el establecimiento del grupo de subconjuntos no codificados, respectivamente codificados que se ha establecido en segundo lugar en el tiempo (solicitud de acceso), se compara cada subconjunto de características, leído a través de un algoritmo insensible a las transformaciones, con el conjunto no codificado de características hasta su coincidencia con una parte de este último, y se clasifica dicho subconjunto codificado en relación con la parte coincidente del conjunto no codificado. Finalmente, una vez que todos los subconjuntos codificados han podido coincidir con partes correspondientes del conjunto no codificado, se emite una instrucción de autorización de acceso para la persona.

En una primera puesta en práctica, se puede, como se muestra en la figura 8, empezar por constituir el conjunto no codificado de características biométricas proporcionado por los medios de tratamiento 4 y transmitir (línea discontinua 7) dicho conjunto a una memoria protegida 8 en la que queda grabado.

Posteriormente, en cada solicitud de autorización de acceso de la persona, se establece, como se ha indicado anteriormente, el grupo de subconjuntos codificados de características biométricas proporcionado por los medios 6. A continuación, el grupo de subconjuntos se transmite en 9 a medios comparadores 10 con objeto de su comparación con el conjunto no codificado de características grabado en la memoria 8.

En función del resultado de la comparación, se emite en 16 hacia la solicitud de acceso una instrucción para autorizar o prohibir el acceso en 11 de la persona.

En otra puesta en práctica preferida, se empieza, como se ilustra en la figura 9, por constituir un grupo de subconjuntos codificados entregado por los medios transformadores algorítmicos 6, y se graba dicho grupo de subconjuntos codificados en una memoria 8.

Posteriormente, en cada solicitud de autorización de acceso, se detectan las características biométricas de la persona, y se constituye en 4 el conjunto no codificado de dichas características. Se extrae entonces de la memoria 8 el grupo de subconjuntos codificados que se envía en 12 hacia la solicitud de acceso, donde se comparan uno por uno los subconjuntos codificados, en medios comparadores 10, con el conjunto no codificado. Finalmente, en función del resultado de la comparación, se emite en 16 una instrucción para autorizar o prohibir el acceso de la persona en 11.

De forma práctica, los medios comparadores 10 son capaces de comparar sucesivamente los subconjuntos codificados a través de los algoritmos que son insensibles a las transformaciones y que el especialista en la materia tiene a su disposición, con el conjunto no codificado de características biométricas hasta la coincidencia de los subconjuntos codificados con partes respectivas del conjunto no codificado.

Dicha comparación no requiere un trabajo demasiado complejo, y todos los medios empleados pueden agruparse en el lugar de la solicitud de acceso, alrededor del sensor 3, con excepción eventualmente de la memoria 8 que puede ser remota geográficamente.

En caso de no coincidencia de un subconjunto codificado con una parte del conjunto no codificado, se puede hacer intervenir un código corrector de error y se emite una autorización de acceso si una proporción predeterminada de n subconjuntos codificados encuentra, tras una corrección eventual, correspondencias respectivas mayoritarias en el conjunto no codificado, mientras se emite una prohibición de acceso si dicha proporción predeterminada de subconjuntos codificados, tras una corrección eventual, no encuentra correspondencias respectivas mayoritarias en el conjunto no codificado. Se pueden evitar así ciertos riesgos de funcionamiento del dispositivo.

La correspondencia de todos los subconjuntos codificados con el conjunto no codificado puede revelarse insuficiente para un reconocimiento exacto de la característica biométrica detectada en la persona. Para compensar dicha insuficiencia, se prevé que tras la puesta en correspondencia de los subconjuntos codificados con el conjunto no co-

dificado, se compara el grupo de subconjuntos codificados y el conjunto no codificado desde el punto de vista de por lo menos una característica adicional que no es detectable, o no detectable en su totalidad en los subconjuntos codificados considerados individualmente y que no se tiene en cuenta en las etapas anteriores. Dichas características adicionales (por ejemplo bifurcaciones, fin de surcos, tipo mayoritario de un lote predefinido de características del conjunto codificado, etc.) consideradas de forma global en el conjunto de la imagen pueden proporcionar una información adicional.

Se puede plantear asimismo detectar las huellas de varios (por ejemplo dos) dedos de la persona y tratar estas dos imágenes. Sin embargo, para no incrementar sobremanera el número de subconjuntos a tratar, se puede prever que si el número de dedos utilizados para la detección es p, se establece para cada dedo un número n/p de subconjuntos con objeto de que el número total de subconjuntos siga igual a n.

Se puede recurrir asimismo a otras características para completar la información. Por ejemplo, las huellas dactilares pueden clasificarse en k tipo generales (en la práctica cinco tipos). Se puede determinar entonces, durante la detección de las características de las huellas dactilares de la persona, el tipo K al que pertenecen y se utiliza el tipo K como información adicional de los subconjuntos codificados.

En los esquemas de las figuras 8 y 9, se ha simbolizado la autorización o la prohibición de acceso, de forma sencilla, como el resultado (SÍ o NO) de la comparación efectuada mediante los medios comparadores 10.

Se puede plantear asimismo una solución más elaborada que consiste en comandar por parte de los medios comparadores 10, en caso de resultado positivo, la generación de un orden complejo, como un código, que se aplica a continuación a medios de comando de acceso. Este modo operativo puede tener una aplicación especialmente interesante para la autentificación seguridad de una persona titular de un código de identificación personal (o código PIN) que la autorice a un acceso. En este caso, los medios propios de la invención pueden, en aplicación de lo que se acaba de indicar, autentificar a la persona, y generar y emitir automáticamente su código de acceso PIN. A tal efecto, en el transcurso de la puesta en práctica del procedimiento de autentificación anteriormente descrito, durante la comparación de los subconjuntos codificados con el conjunto no codificado a través de los algoritmos insensibles a las transformaciones, se detecta, con la ayuda de dichos algoritmos, la combinación de transformaciones experimentadas anteriormente por los subconjuntos codificados.

Se compara entonces la combinación así encontrada con una combinación guardada en memoria en relación con un código PIN y, en caso de identidad, se emite el código PIN para comandar la autorización de acceso de la persona.

Se puede plantear que la persona no deba efectuar intervención alguna a nivel de la generación del código PIN y que éste, que se genera automáticamente, pueda ser uno cualquiera y tan complejo como se desee. Especialmente, se puede hacer que el código PIN sea la propia combinación encontrada.

A título de ejemplo, durante la comparación de cada subconjunto codificado con el conjunto no codificado, los algoritmos insensibles a las transformaciones permiten hacer más discreta cada transformación en el conjunto E de las posibles transformaciones; a cada parte del conjunto no codificado seleccionado se asocia un índice i del conjunto E correspondiente a la formación identificada. Una clave intermedia puede construirse entonces mediante combinación del índice i del subconjunto y de la transformación que le ha sido aplicada, de este modo, considerando seis subconjuntos, doce señuelos y diez transformaciones por subconjunto, el número de combinaciones es

$$C^{18}_{6} \times 10^{6} = 18564000000.$$

Sin embargo, en la práctica, se limita este número de combinaciones, limitando el número de posibles transformaciones o utilizando códigos correctores de errores para incrementar la fiabilidad del sistema. Por ejemplo, sobre la base de las tres transformaciones P, R y H indicadas el número de combinaciones es

$$C^{18}_{6} \times 3^{6} = 13153156.$$

Para incrementar la calidad de información, se calcula una clave final resultante de la concatenación de dicha clave intermedia y otros datos ligados a la clasificación de la huella dactilar, la frecuencia de sus surcos, y otras características extraídas de las minucias (por ejemplo la valencia y la curvatura).

Finalmente, se aplica el código corrector de error a dicha clave final, y se obtiene un código final que puede hacer oficio de código PIN.

En este caso, la forma compleja del código PIN provoca que la persona no deba necesariamente memorizarlo.

Por lo tanto, el dispositivo de la figura 9 anteriormente descrito queda completado, como se ilustra en la figura 10, para poner en práctica lo expuesto anteriormente, con medios generadores 13 situados bajo la dependencia de los medios comparadores 10 capaces de elaborar un código PIN que se emite a continuación para autorizar el acceso en 16.

También es posible plantear que se detecte la combinación de transformaciones experimentadas anteriormente por los subconjuntos codificados con la ayuda de los algoritmos insensibles a las transformaciones y que, a continuación, como se ilustra en la figura 11, se busque dicha combinación en una tabla memorizada 14 que encierra, por una parte, una lista de combinaciones de posibles transformaciones y, en frente, una lista de códigos PIN, estando las transformaciones y los códigos PIN en relación biunívoca. A continuación de lo cual, se anota en 15 el código PIN en relación con la combinación encontrada, y se utiliza dicho código PIN para comandar en 16 la autorización de acceso de la persona.

Los dos procedimientos que se acaban de describir con relación a las figuras 10 y 11 son especialmente interesantes, ya que dejan la posibilidad de remediar una disfunción del dispositivo. A tal efecto, se prevé que la persona disponga de un código PIN que puede ser distinto del código PIN generado automáticamente por uno de los dispositivos de las figuras 10 u 11, o que puede ser el mismo en el caso de la figura 11. En estas condiciones, la solicitud de acceso puede efectuarse manualmente, por ejemplo por medio de un teclado auxiliar, por la persona directamente con la ayuda de su propio código PIN si está autorizada al término de una puesta en práctica no válida del proceso de autentificación y de generación automática del código PIN.

REIVINDICACIONES

1. Procedimiento de autentificación con seguridad de una persona para autorizar a ésta a un acceso, mediante la detección de características biométricas de dicha persona,

caracterizado porque incluye las etapas que consisten en:

- establecer una imagen codificada de características biométricas de la persona poniendo en práctica las siguientes etapas:

  - se detectan (3) características biométricas (1) de la persona y se establece (4) un conjunto (2) de dichas características biométricas,
  - se divide (5) dicho conjunto de características en un número n de subconjuntos de características (A-F), y
  - se aplica (6) a por lo menos uno de los subconjuntos o a cada uno de por lo menos algunos subconjuntos por lo menos una transformación geométrica del tipo traslación-permuta (P), rotación (R), homotecia (H),

gracias a lo cual se constituye una imagen codificada de dichas características biométricas, que está constituida por un grupo de n subconjuntos transformados que representa una combinación de transformaciones entre todas las combinaciones de posibles transformaciones en los n subconjuntos de características;

- con un desfase temporal bien antes, bien después del establecimiento de la imagen codificada mencionada:

  - detectar (3) dichas características biométricas (1) de la persona y establecer (4) un conjunto no codificado (2) de dichas características biométricas,
  - mantener en memoria (8) el grupo de subconjuntos de características codificados, respectivamente el conjunto no codificado establecido en primer lugar en el tiempo,
  - durante el establecimiento del conjunto no codificado, respectivamente del grupo de subconjuntos codificados de características establecido en segundo lugar en el tiempo, comparar (10) cada subconjunto codificado de características, leído a través de un algoritmo insensible a las transformaciones, con el conjunto no codificado de características hasta su coincidencia con una parte de este último y clasificar dicho subconjunto codificado en relación con la parte coincidente del conjunto no codificado; y

- cuando todos los subconjuntos codificados de características han podido ponerse en coincidencia con las partes correspondientes del conjunto no codificado de características, emitir (16) una instrucción de autorización de acceso (11) para la persona.

2. Procedimiento de autentificación con seguridad, según la reivindicación 1, **caracterizado** porque el grupo de subconjuntos de características (A-F) es transformado por lo menos una primera vez, y porque dicha primera transformación consiste en una traslación-permuta (P) aplicada a por lo menos una pareja de subconjuntos de características.

3. Procedimiento de autentificación con seguridad, según la reivindicación 2, **caracterizado** porque se efectúa una segunda transformación en el grupo de subconjuntos de características resultante de la primera transformación, y porque la segunda transformación consiste en una rotación (R), respectivamente una homotecia (H), efectuada en por lo menos un subconjunto o en cada uno de por lo menos ciertos subconjuntos de dicho grupo resultante de la primera transformación (P).

4. Procedimiento de autentificación con seguridad, según la reivindicación 3, **caracterizado** porque se efectúa una tercera transformación en el grupo de subconjuntos de características resultante de la segunda transformación, y porque la tercera transformación consiste en una homotecia (H), respectivamente una rotación (R), efectuada en por lo menos un subconjunto o en cada uno de por lo menos algunos subconjuntos de dicho grupo resultante de la segunda transformación (R, respectivamente H).

5. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones anteriores, **caracterizado** porque se añade al grupo de subconjuntos de características, antes de la primera transformación y/o entre dos transformaciones y/o después de la última transformación, por lo menos un falso subconjunto de características (señuelo) (L), gracias a lo cual se incrementa el número de combinaciones de posibles transformaciones.

6. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque:

- se empieza por constituir (4) el conjunto no codificado de características biométricas que se graba en una memoria protegida (8),

- en cada solicitud de acceso de la persona, se establece (3-6) el grupo de subconjuntos codificados de características biométricas y se transmite dicho grupo de subconjuntos codificados a la memoria, para comparación (10) de éste con el conjunto no codificado de características conservado en memoria,

- en función del resultado de la comparación, se emite (16) una instrucción hacia la solicitud de acceso para autorizar o prohibir el acceso (11) de la persona.

7. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 5, **caracterizado** porque:

- se empieza por detectar las características biométricas de la persona y por constituir (6) el grupo de subconjuntos codificados de características biométricas que se graba en una memoria (8),

- en cada solicitud de acceso de la persona, se detectan (3) las características biométricas de la persona y se constituye (4) el conjunto no codificado de sus características biométricas,

- se extrae de la memoria el grupo de subconjuntos codificados de características que se transmite hacia la solicitud de acceso, donde es comparado (10) con el conjunto no codificado, y

- en función del resultado de la comparación, se emite (16) una instrucción para autorizar o prohibir el acceso (11) de la persona.

8. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 7, **caracterizado** porque se comparan (10) sucesivamente los subconjuntos codificados de características, a través de los algoritmos insensibles a las transformaciones, con el conjunto no codificado de características biométricas hasta su coincidencia respectiva de los subconjuntos codificados con partes respectivas del conjunto no codificado.

9. Procedimiento de autentificación con seguridad, según la reivindicación 8, **caracterizado** porque en caso de no coincidencia de un subconjunto codificado de características con una parte del conjunto de características no codificado, se hace intervenir un código corrector de error, y porque se emite una autorización de acceso si una proporción predeterminada de los $\underline{n}$ subconjuntos codificados, tras la eventual corrección de error, encuentra correspondencias respectivas en el conjunto no codificado, mientras que se emite una prohibición de acceso si dicha proporción predeterminada de subconjuntos codificados, tras la corrección de un eventual error, no encuentra correspondencias respectivas en el conjunto no codificado.

10. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque tras la correspondencia de los subconjuntos codificados con el conjunto no codificado, se compara el grupo de subconjuntos codificados y el grupo no codificado desde el punto de vista de por lo menos una característica adicional no detectable en los subconjuntos codificados individuales y no tenidos en cuenta en las etapas anteriores

y sólo se emite una autorización de acceso en caso de correspondencia mayoritaria asimismo en dicha característica adicional.

11. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 10, **caracterizado** porque las características biométricas son las de las huellas dactilares (1) de por lo menos un dedo de la persona.

12. Procedimiento de autentificación con seguridad, según la reivindicación 11, **caracterizado** porque las características biométricas son las de las huellas dactilares de varios dedos de la persona.

13. Procedimiento de autentificación con seguridad, según la reivindicación 12, **caracterizado** porque dado que el número de dedos utilizado es $\underline{p}$, se establece para cada dedo un número $\underline{n}/\underline{p}$ de subconjuntos de características biométricas, con objeto de que el número total de subconjuntos de características siga igual a $\underline{n}$.

14. Procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 10 a 13, **caracterizado** porque dado que las huellas dactilares de los dedos de las manos pueden clasificarse en $\underline{k}$ tipos generales, se determina, durante la detección de las características de las huellas dactilares de la persona, el tipo $\underline{K}$ al que pertenecen, y se utiliza el tipo K como información adicional de los subconjuntos codificados.

15. Procedimiento de autentificación con seguridad de una persona titular de un código de identificación personal PIN que la autoriza a un acceso, **caracterizado** porque:

- se pone en práctica el procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 14;

- en el transcurso de la comparación (10) de los subconjuntos codificados con el subconjunto no codificado a través de los algoritmos insensibles a las transformaciones, se detecta, con la ayuda de dichos algoritmos, la combinación de las transformaciones experimentadas anteriormente por los subconjuntos codificados;

- se elabora (13), especialmente a partir de la combinación de las transformaciones detectadas mediante los algoritmos insensibles a las transformaciones, una clave que se considera como código PIN asignado a la persona; y

- finalmente se utiliza el código PIN así elaborado para comandar (16) la autorización de acceso (11) de la persona;

gracias a lo cual el código PIN puede ser una función cualquiera.

16. Procedimiento de autentificación con seguridad de una persona titular de un código de identificación personal PIN que la autoriza a un acceso,

caracterizado porque:

- se pone en práctica el procedimiento de autentificación con seguridad, según una cualquiera de las reivindicaciones 1 a 14;

- en el transcurso de la comparación (10) de los subconjuntos codificados con el subconjunto no codificado a través de los algoritmos insensibles a las transformaciones, se detecta, con la ayuda de dichos algoritmos, la combinación de las transformaciones experimentadas anteriormente por los subconjuntos codificados;

- se busca (15) la combinación así encontrada de las transformaciones en una tabla (14) que encierra, por una parte, una lista de códigos PIN que están en relación biunívoca, y se anota el código PIN en relación con la combinación encontrada, y

- finalmente se utiliza el código PIN seleccionado para comandar (16) la autorización de acceso (11) de la persona.

17. Procedimiento de autentificación con seguridad, según la reivindicación 15, **caracterizado** porque la persona dispone de un código PIN, y porque la solicitud de acceso puede efectuarse manualmente por parte de la persona directamente con la ayuda de su propio código PIN si está autorizada a ello al término de una puesta en práctica no válida del procedimiento de autentificación con seguridad automático, según la reivindicación 15 o 16.

18. Dispositivo de autentificación con seguridad de una persona para autorizar a ésta a un acceso, mediante la detección de por lo menos una característica biométrica de dicha persona, para la puesta en práctica del procedimiento según una cualquiera de las reivindicaciones 1 a 14, **caracterizado** porque incluye:

- un dispositivo de codificación de una imagen detectada de características biométricas de una persona, que incluye:

  - medios captores (3) capaces de detectar características biométricas de una persona,
  - medios de tratamiento (4), situados bajo la dependencia de los medios sensores, capaces de establecer un conjunto de dichas características biométricas detectadas,
  - medios de división (5) capaces de dividir dicho conjunto en n subconjuntos de características biométricas,
  - medios transformadores algorítmicos (6) capaces de transformar geométricamente un subconjunto mediante traslación-permuta (P), rotación (R), homotecia (H) para proporcionar un subconjunto transformado,

gracias a lo cual el dispositivo de codificación proporciona, de un conjunto no codificado de características biométricas, un conjunto codificado constituido por subconjuntos transformados;

- medios de memorización (8) para grabar los subconjuntos codificados de características biométricas o el conjunto no codificado de características biométricas;

- medios de comparación (10) capaces de comparar sucesivamente cada subconjunto codificado con el conjunto no codificado, incluyendo dichos medios comparadores algoritmos insensibles a las transformaciones experimentadas por los subconjuntos codificados; y

- medios (13, 16) generadores de una instrucción de autorización situados bajo la dependencia de dichos medios de comparación y capaces de generar una instrucción de autorización sólo cuando los medios comparadores han establecido una correspondencia mayoritaria de los subconjuntos codificados en el conjunto no codificado.

19. Dispositivo de autentificación con seguridad, según la reivindicación 18, **caracterizado** porque dichos medios transformadores algorítmicos son capaces de efectuar por lo menos una primera transformación del tipo traslación-permuta (P) y, en su caso, una segunda y tercera transformación del tipo rotación (R) u homotecia (H) respectivamente.

20. Dispositivo de autentificación con seguridad, según la reivindicación 18 o 19, **caracterizado** porque incluye además medios generadores de falsos subconjuntos (GL) capaces de generar por lo menos un falso subconjunto e introducirlo, como señuelo, entre los subconjuntos de características biométricas, lo que incrementa el número de subconjuntos en el conjunto codificado.

21. Dispositivo de autentificación con seguridad, según una cualquiera de las reivindicaciones 18 a 20, siendo dicha persona titular de un código de identificación personal PIN que la autoriza a un acceso, **caracterizado** porque los medios (13, 16) generadores de una instrucción de autorización son capaces, a partir de las transformaciones que los algoritmos insensibles a las transformaciones han detectado en los subconjuntos codificados, de determinar la combinación correspondiente de las transformaciones y de elaborar a partir de dicha combinación una clave utilizable como código PIN.

22. Dispositivo de autentificación con seguridad, según una cualquiera de las reivindicaciones 18 a 20, siendo dicha persona titular de un código de identificación personal PIN que la autoriza a un acceso, **caracterizado**

- porque incluye segundos medios de memorización (14) que encierran una tabla de relaciones biunívocas entre una multiplicidad de combinaciones entre las que figura la combinación particular de las transformaciones experimentadas por los subconjuntos codificados y una multiplicidad equivalente de códigos PIN entre los que figura, en correspondencia con dicha combinación particular, el código PIN asignado a la persona,

- porque los algoritmos incluidos en los medios de comparación son capaces de detectar las transformaciones experimentadas por los subconjuntos codificados y de determinar la combinación de dichas transformaciones,

- porque incluye segundos medios comparadores (15) capaces de comparar la combinación de las transformaciones restituida mediante los algoritmos y las combinaciones contenidas en la tabla de los segundos medios de memorización, y

- porque los medios generadores de una instrucción de autorización (16) están situados bajo la dependencia de dichos segundos medios comparadores (15) y son capaces de generar el código PIN correspondiente a la combinación detectada a destino de un órgano de autorización de acceso (11) comandado por dicho PIN.

23. Dispositivo de autentificación con seguridad, según la reivindicación 21 o 22, **caracterizado** porque incluye además medios de introducción manual del o de un código PIN por parte de la persona, y porque los medios de introducción manual están situados bajo la dependencia de dichos medios generadores para inhibirse cuando el dispositivo es capaz de generar automáticamente la búsqueda y la emisión del código PIN y para activarse cuando no es posible la generación automática del código PIN.

24. Dispositivo de autentificación con seguridad, según una cualquiera de las reivindicaciones 18 a 23, **caracterizado** porque los medios sensores son capaces de detectar las huellas dactilares de por lo menos un dedo de la persona.

FIG.1A

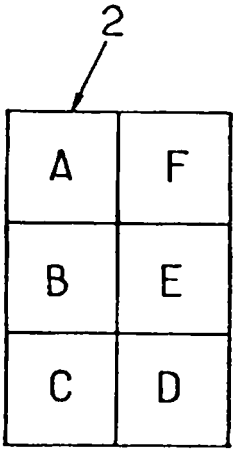

FIG.1B.

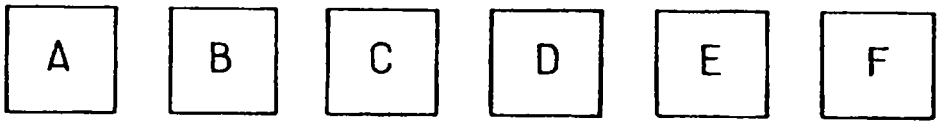

FIG.2.

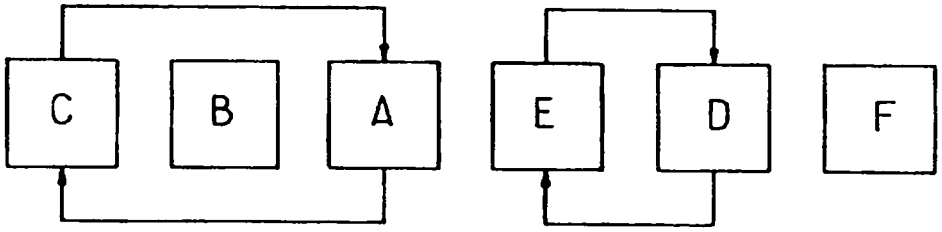

FIG.3.

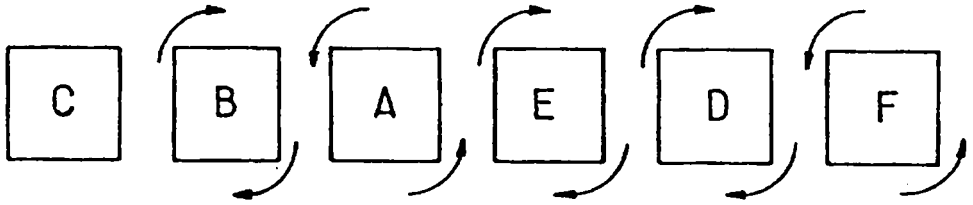

FIG.4.

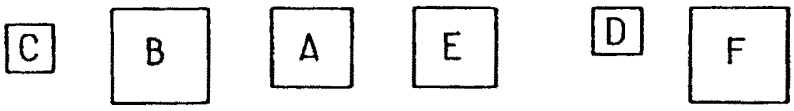

FIG. 5.

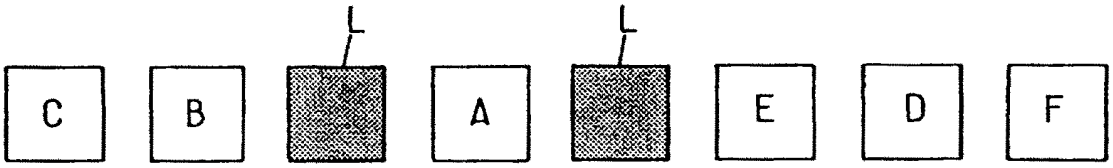

FIG. 6.

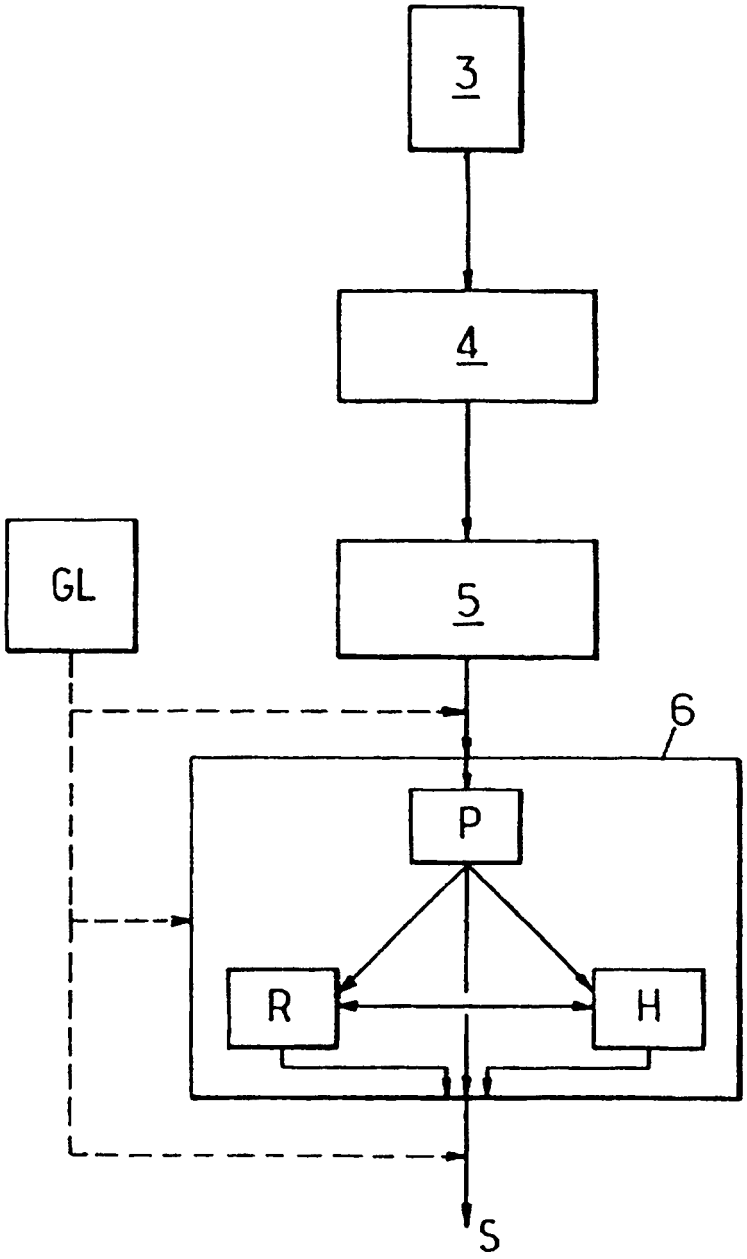

FIG. 7.

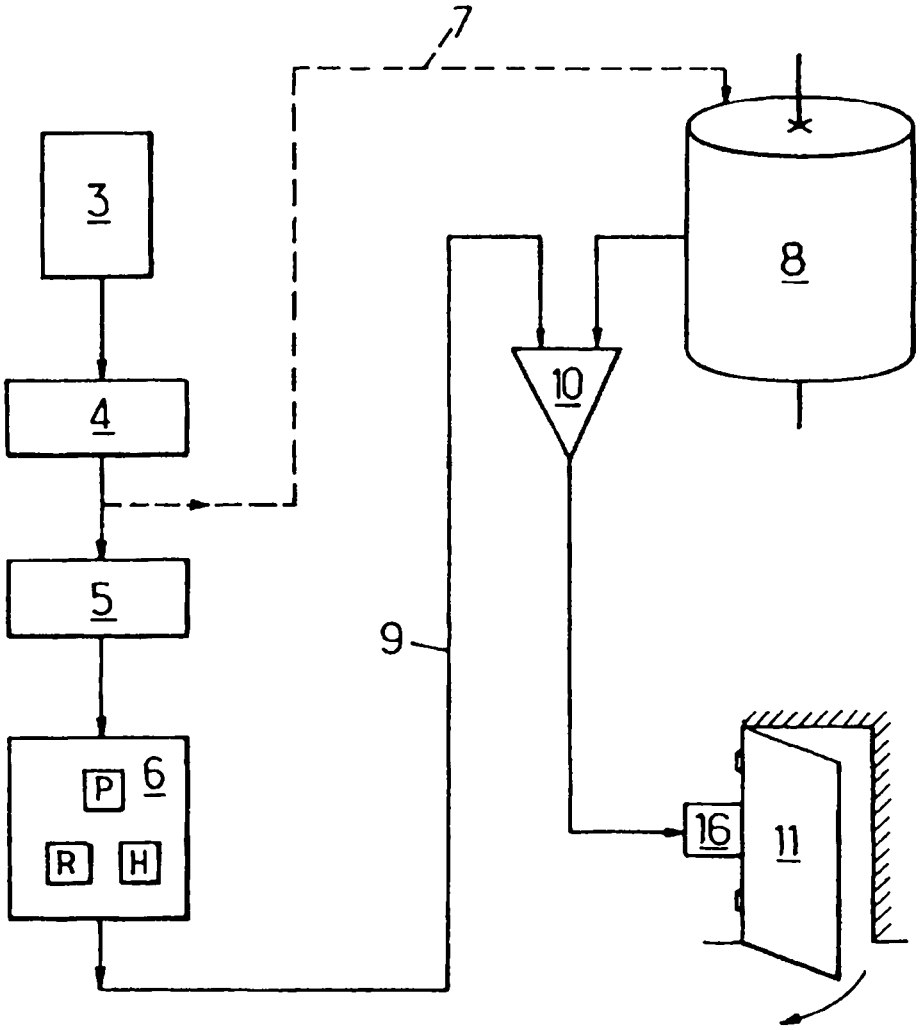

FIG.8.

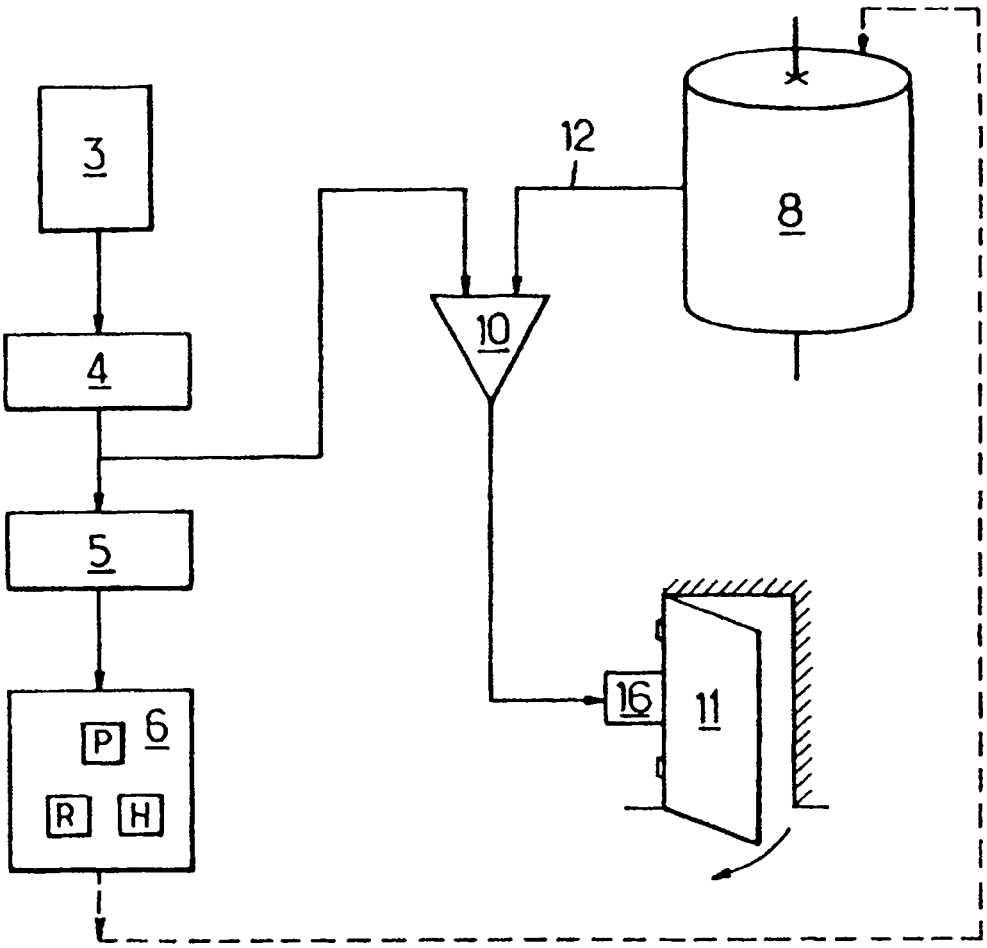

FIG.9.

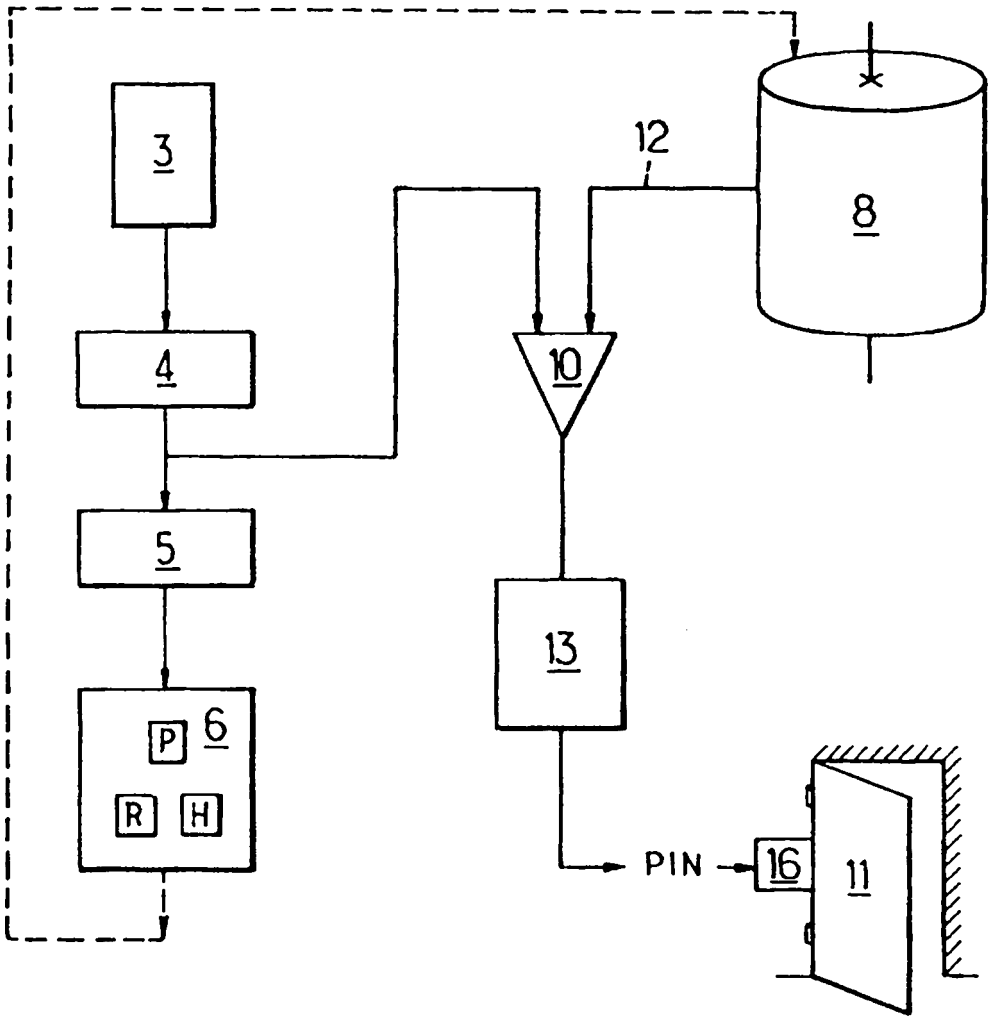

FIG. 10.

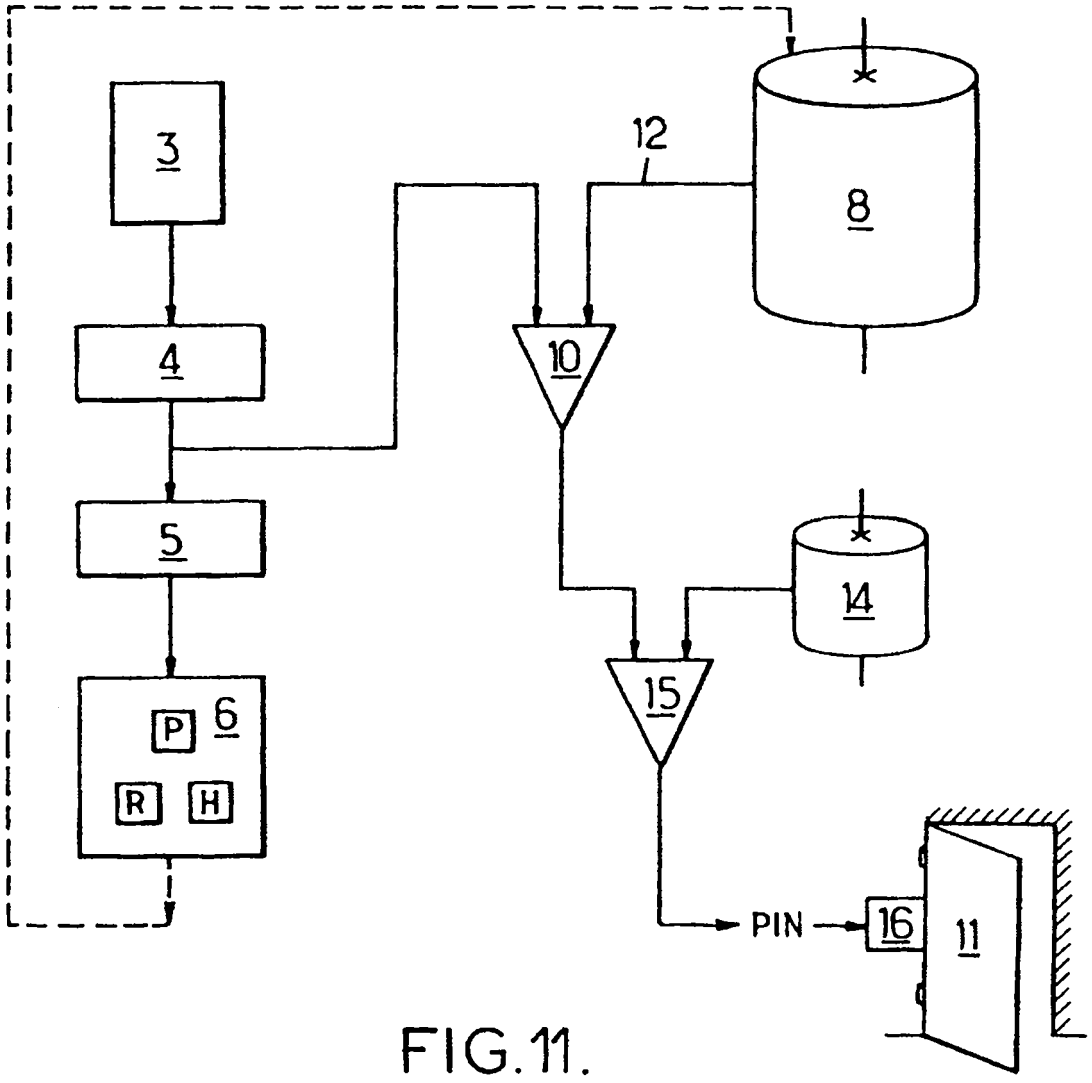

FIG.11.