(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 385 608**

(51) Int. CI.:
G07C 9/00 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07730988 .8**
(96) Fecha de presentación: **15.02.2007**
(97) Número de publicación de la solicitud: **1997064**
(97) Fecha de publicación de la solicitud: **03.12.2008**

(54) Título: **Protección de un control de acceso biométrico**

(30) Prioridad:
03.03.2006 FR 0601933

(45) Fecha de publicación de la mención BOPI:
27.07.2012

(45) Fecha de la publicación del folleto de la patente:
27.07.2012

(73) Titular/es:
MORPHO
27, RUE LEBLANC
75015 PARIS, FR

(72) Inventor/es:
CHABANNE, Hervé

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Protección de un control de acceso biométrico.

La presente invención concierne al control de acceso y, más en particular, al control de acceso basado en un análisis biométrico, es decir, un análisis de características físicas individuales.

Con objeto de garantizar la seguridad de determinada información, se puede poner en práctica un control de acceso de las personas basándose en un análisis biométrico de las personas. Estos controles pueden estar basados en un análisis de características morfológicas, tales como, por ejemplo, de las huellas dactilares, de la retina, del iris o del rostro, e incluso en un análisis de características del comportamiento, tales como por ejemplo de las características relativas a una dinámica de la firma, o incluso a una dinámica de tecleo en un teclado. Estos controles pueden estar basados asimismo en una combinación de esos diferentes tipos de análisis.

La puesta en práctica de tales controles de acceso generalmente tiene por objetivo la protección de información a la que sólo está autorizado a acceder un grupo definido de personas. Esa información puede estar ubicada, por ejemplo, en un sitio físico y, en tal caso, el control de acceso consiste en controlar el acceso físico de una persona a ese sitio. También puede ser accesible mediante un sistema informático y, en tal caso, el control de acceso consiste en controlar el acceso a ese sistema informático.

Cualquiera que sea el tipo de información y el tipo de acceso a esa información, un sistema de control biométrico generalmente comprende un servidor de control de acceso que gestiona una base de datos que almacena unas señales de comparación respectivamente correspondientes a unas características propias de las personas autorizadas a acceder a esa información. Asimismo comprende una pluralidad de sensores de control de acceso que están adaptados para captar una señal biométrica que ha de controlarse con relación a una persona que pretende acceder a la información y para cooperar con un dispositivo de transmisión al objeto de transmitir al servidor de control la señal biométrica captada. Por ejemplo, cuando el control de acceso biométrico se basa en características de una huella, las señales de comparación corresponden a imágenes digitales de huellas del grupo de personas autorizadas a acceder a la información o personas autorizadas en lo sucesivo. Así, en un control de acceso de una persona, esta última coloca su dedo sobre uno de los sensores de control de acceso del sistema. Se capta entonces una imagen de la huella de esa persona, que seguidamente se transmite en forma de una señal biométrica al servidor de control, el cual a continuación está en disposición de comparar la señal biométrica captada recibida y las señales de comparación almacenadas en la base de datos, con el fin de determinar si la persona que pretende acceder a la información forma parte del grupo de personas autorizadas a hacerlo.

Una señal biométrica comprende características individuales que no o prácticamente no evolucionan con el tiempo. Así pues, es importante proteger el carácter confidencial de tales señales biométricas en tales sistemas de control de acceso.

A tal efecto, el documento US 6 836 554 da a conocer un sistema de control en el que las señales de comparación y las señales biométricas captadas que han de controlarse son almacenadas y manipuladas en una forma transformada, obtenida mediante aplicación a la señal biométrica captada de una función de transformación no reversible. Más concretamente, con el fin de que el servidor de control aprenda las señales de comparación con las que se compararán las señales recibidas en un control de acceso, el sensor capta, en una fase de inicialización, una señal biométrica de una persona autorizada, seguidamente esa señal captada es transformada mediante aplicación de una función de transformación correspondiente a la persona controlada, antes de ser enviada, así transformada, con destino al servidor de control. Este último la almacena con el fin de poder efectuar un control de acceso mediante comparación de la señal recibida y de las señales almacenadas.

De esta manera, el servidor almacena directamente las señales de comparación en una forma transformada que corresponde a la forma según la cual recibe asimismo las respectivas señales captadas.

Así, un potencial atacante tan sólo puede interceptar una señal biométrica transformada, puesto que las señales almacenadas e intercambiadas lo son en una forma transformada. Además, a partir de la forma transformada de una señal biométrica interceptada, un potencial atacante no está capacitado para recuperar la señal biométrica original, puesto que la función de transformación que se ha aplicado presenta un carácter no reversible.

En cambio, si un potencial atacante recupera una señal de comparación de la base de datos o incluso intercepta una señal biométrica que ha de controlarse en el transcurso de su transmisión entre un sensor y el servidor de control, entonces está capacitado para reproducir nuevamente esa señal biométrica transformada interceptada, en cualquier contexto, con el fin de acceder a la información protegida.

El documento US 6 836 554 propone, en el caso en que la seguridad de semejante sistema se ve comprometida por un ataque así basado en una nueva reproducción de señal biométrica transformada, sustituir la función de transformación correspondiente a la señal biométrica transformada por una nueva función de transformación.

No obstante, en semejante caso, se prevé entonces que el servidor aprenda la nueva señal de comparación

correspondiente a una persona autorizada, como en la fase de inicialización descrita más arriba. De ello se deriva una complejidad y una pesadez de tal gestión de cambio de función de transformación, puesto que se requiere entonces un nuevo registro de la señal de comparación.

El documento WO02/095657 propone efectivamente un procedimiento para evitar la nueva reproducción de una señal biométrica transmitida al utilizar funciones de un sólo uso, pero estas funciones son reversibles.

La presente invención trata de subsanar los inconvenientes antedichos.

Un primer aspecto de la presente invención propone un procedimiento de control de acceso en un sistema de control de acceso que comprende un servidor de control de acceso adaptado para controlar un acceso, al menos un sensor de señal biométrica; y un dispositivo de interfaz adaptado para estar relacionado, por una parte, con el servidor de control y, por otra parte, con el sensor.

El acceso controlado se autoriza a al menos una persona que tiene asociada una señal de referencia que comprende información biométrica correspondiente.

El servidor de control y el dispositivo de interfaz, por una parte, gestionan un parámetro común que toma valores diferentes con el paso del tiempo y, por otra parte, almacenan respectivamente una primera y una segunda función de transformación no reversible, siendo dichas funciones primera y segunda parametrizadas en función al menos del parámetro común.

El procedimiento comprende las siguientes etapas:

/a/ a nivel del sensor, captar una señal biométrica y proporcionar la señal biométrica captada al dispositivo de interfaz;

/b/ a nivel del dispositivo de interfaz, obtener una señal biométrica transformada aplicando la primera función de transformación a un elemento de entre un grupo que comprende al menos una característica derivada de dicha señal biométrica captada y dicha señal biométrica captada; y transmitir la señal biométrica transformada con destino al servidor de control;

/c/ a nivel del servidor de control, efectuar una comparación de la señal biométrica transformada con al menos una señal de comparación, correspondiendo la señal de comparación a una señal resultante de la aplicación de la segunda función de transformación a una señal inicial derivada de la señal de referencia; y

/d/ basándose en la comparación, decidir si se autoriza un acceso.

En virtud de estas disposiciones, toda vez que la primera función de transformación aplicada a la señal biométrica captada y la segunda función de transformación aplicada a la señal inicial derivada de la señal de referencia son ambas determinadas en función de un parámetro común cuyo valor evoluciona en función del tiempo, se puede evitar ventajosamente un ataque basado en la nueva reproducción de una señal biométrica transformada interceptada. En efecto, con cada cambio de valor del parámetro común, la función de transformación aplicada puede corresponder así a una transformación diferente de la que acaba de ser aplicada para el control precedente. Esta función de transformación parametrizada de manera diferente se determina a la vez por parte de la persona que ha de controlarse y por parte del servidor de control. Consecuentemente, para una misma persona controlada en momentos diferentes, son procesadas según tal control señales biométricas transformadas o deformadas de manera diferente, con lo que es imposible atacar tal procedimiento basándose en la nueva reproducción de una señal biométrica transformada interceptada.

En semejante contexto, un cambio de transformación que haya de aplicarse a una imagen captada es sencillo en su puesta en práctica y no precisa de un nuevo registro de una señal biométrica de referencia cada vez, como es el caso en la técnica anterior.

La primera función de transformación está adaptada para ser aplicada bien sea directamente a la señal biométrica captada por el sensor, o bien para ser aplicada a una o varias características biométricas derivadas de la señal biométrica captada, es decir, extraídas de la señal biométrica captada, por ejemplo mediante la utilización de un algoritmo conocido por el experto en la materia.

La señal inicial o las señales iniciales obtenidas en el lado del servidor corresponden ya sea a señales directamente captadas, o bien a características extraídas de señales biométricas captadas, en función del elemento del grupo en cuestión al que se aplica la primera función de transformación.

En una forma de realización de la presente invención, es posible determinar una evolución del parámetro común que permite modificar, para cada control de acceso, la transformación que ha de aplicarse a la señal biométrica captada mediante el sensor a partir de una persona. Se puede prever en ciertos casos una evolución menos rápida de los valores del parámetro común. Esta evolución del parámetro común se puede determinar ventajosamente en función del nivel de seguridad que se pretenda alcanzar en el sistema de control en cuestión.

En una forma de realización de la presente invención, los valores del parámetro común para el servidor de control y para el dispositivo de interfaz son función de los valores de un contador, gestionado a nivel del dispositivo de interfaz y del servidor, del número de señales biométricas transformadas que son transmitidas y recibidas respectivamente por el dispositivo de interfaz y el servidor de control.

En este contexto, los contadores respectivamente gestionados por el servidor y por el sensor presentan valores sensiblemente síncronos y, por tanto, pueden ser utilizados ventajosamente para determinar el valor del parámetro común. Se puede prever que, regularmente, después de N señales biométricas captadas y transmitidas desde el sensor con destino al servidor, el parámetro común se incrementa, siendo N un número entero que se puede definir ventajosamente en función del nivel de seguridad perseguido para tal control de acceso.

En una variante, al estar sincronizados el servidor de control de acceso y el sensor en una referencia temporal común, los valores del parámetro común son función de esa referencia temporal común.

Así, se puede prever incrementar el parámetro común después de cada período de tiempo T, pudiendo definirse este período T en función del nivel de seguridad perseguido en el sistema de control en cuestión.

Los valores del parámetro común pueden corresponder a valores registrados a nivel del dispositivo de interfaz. En tal caso, cada nuevo valor del parámetro común, utilizado para parametrizar la función de transformación, se transmite desde el dispositivo de interfaz al servidor de control.

En una forma de realización de la presente invención, el sistema de control de acceso controla el acceso a una pluralidad de tipos de aplicaciones, como por ejemplo, un acceso físico en un sitio físico, un acceso a una base de datos informáticos en una red informática y un acceso a un servicio bancario asimismo en una red informática. En semejante contexto, con dicha pluralidad de tipos de aplicaciones se asocia respectivamente una pluralidad de pares, conformados por una parte por una primera función de transformación no reversible a nivel del dispositivo de interfaz y, por otra parte, por una segunda función de transformación no reversible a nivel del servidor de control. Así, ventajosamente, se puede obtener un gran nivel de seguridad sin modificar por ello con cada control la parametrización de la función de transformación, puesto que cada aplicación de diferente tipo se puede controlar entonces poniendo en práctica una función de transformación diferente. Consecuentemente, un potencial atacante, si intercepta una señal transformada que va a controlarse, no está capacitado para 'reproducir nuevamente' esa señal transformada interceptada para acceder a una aplicación controlada de otro tipo del sistema.

En este contexto, se puede prever además que la pluralidad de pares de funciones de transformación no reversibles se asocia respectivamente a parámetros comunes diferentes.

La señal inicial puede comprender la señal de referencia. En tal caso, la aplicación de la primera y la aplicación de la segunda función de transformación parametrizadas no reversibles son equivalentes.

En una forma de realización de la presente invención, la señal inicial derivada de la señal de referencia, correspondiente a la o a las personas autorizadas, se obtiene mediante aplicación de una función de transformación inicial no reversible a la señal de referencia, de modo que la señal inicial es una señal previamente transformada. En este contexto, la primera función de transformación equivale a una combinación de la segunda función de transformación y de la función de transformación inicial.

Al proceder de esta manera, las señales biométricas de referencia relativas a las personas para las cuales el acceso está autorizado se almacenan en una forma ya transformada previamente. Semejante forma de realización permite proteger la confidencialidad de las características biométricas, las cuales, por su parte, no pueden ser modificadas para una persona dada.

En una forma de realización de la presente invención, se asocia un identificador con el dispositivo de interfaz y/o con la al menos una persona a la que se autoriza el acceso y el servidor de control gestiona una asociación de la al menos una señal de comparación con dicho identificador de esa persona. En tal caso, el procedimiento puede comprender además, antes de la etapa /c/, las siguientes etapas:

- obtener, a nivel del dispositivo de interfaz, un identificador correspondiente a la señal biométrica captada;
- transmitir al servidor de control dicho identificador; y
- a nivel del servidor de control, recuperar la señal de comparación asociada a dicho identificador recibido.

Así, en virtud de la gestión por parte del servidor de control de una asociación de una señal de comparación correspondiente a una persona para la que está autorizado el acceso y un identificador de esa persona y/o del dispositivo de interfaz, el servidor está en disposición de recuperar de manera más eficaz la señal de comparación de su base de datos en función del identificador que recibe de la persona que está controlándose en el sistema de control.

En tal forma de realización de la presente invención, el sistema de control puede ser utilizado entonces como

sistema de autenticación de una persona. En efecto, en tal puesta en práctica, el servidor está en disposición de autenticar a la persona que se está controlando basándose en el identificador y en la señal biométrica transformada recibida.

El sistema de control según una forma de realización de la presente invención puede ser utilizado asimismo como sistema de identificación. En tal caso, la señal inicial obtenida por el servidor está asociada a un identificador de la persona para la que está autorizado el acceso. Así, el servidor está en disposición de identificar a una persona basándose en una señal biométrica transformada. En efecto, cuando el servidor decide que la señal biométrica transformada recibida corresponde a una señal inicial, entonces está en disposición de recuperar un identificador de la persona correspondiente que se está controlando y, con ello, de identificar a esa persona.

Ventajosamente, en el caso de una identificación en la que las transformaciones aplicadas a las imágenes captadas cambian con cada nuevo control de acceso de una misma persona, la información que transita entre el lado del usuario y el servidor no permite a un potencial atacante detectar cuándo se identifica a una misma persona mediante un sistema según la presente invención.

Un segundo aspecto de la presente invención propone un dispositivo de interfaz en un sistema de control de acceso que comprende, por una parte, además un servidor de control de acceso adaptado para controlar un acceso y, por otra parte, al menos un sensor de señal biométrica. El acceso se autoriza a al menos una persona que tiene asociada una señal de referencia que comprende información biométrica correspondiente. El dispositivo de interfaz puede comprender:

- una unidad de gestión adaptada para gestionar, por una parte, un parámetro, común con el servidor de control, que toma valores diferentes con el paso del tiempo y, por otra parte, una función de transformación no reversible, siendo dicha función parametrizada en función de al menos dicho parámetro común;

- una primera unidad de interfaz adaptada para recibir una señal biométrica captada desde el sensor;

- una unidad de transformación adaptada para transformar una señal biométrica captada en una señal biométrica transformada aplicando la función de transformación a un elemento de entre un grupo que comprende al menos una característica derivada de dicha señal biométrica captada y dicha señal biométrica captada; y

- una segunda unidad de interfaz adaptada para cooperar con un dispositivo de transmisión (15) adaptado para transmitir una señal biométrica transformada por la unidad de transformación con destino al servidor de control.

Los valores del parámetro común pueden evolucionar tal como se ha especificado según el primer aspecto de la presente invención.

En una forma de realización de la presente invención, la segunda unidad de interfaz del dispositivo de interfaz está adaptada para cooperar con un dispositivo de transmisión con el fin de transmitir la señal transformada, pudiendo hallarse este dispositivo de transmisión ya sea comprendido en el dispositivo de interfaz, o bien incluso exterior a este dispositivo de interfaz.

Un tercer aspecto de la presente invención propone un sensor de señal biométrica que comprende un dispositivo de interfaz según el segundo aspecto de la presente invención.

Este sensor puede comprender el dispositivo de transmisión de la señal biométrica transformada con destino al servidor de control.

Un cuarto aspecto de la presente invención propone un servidor de control de acceso en un sistema de control de acceso que comprende además al menos un sensor de señal biométrica y un dispositivo de interfaz adaptado para estar relacionado, por una parte, con el servidor de control y, por otra parte, con el sensor.

El servidor de control puede comprender:

- una unidad de interfaz adaptada para recibir una señal biométrica transformada proporcionada por dicho dispositivo de interfaz;

- una unidad de gestión adaptada para gestionar, por una parte, un parámetro, común con el dispositivo de interfaz, que toma valores diferentes con el paso del tiempo y, por otra parte, una función de transformación no reversible, siendo dicha función de transformación parametrizada en función de al menos dicho parámetro común a dicha señal inicial;

- una unidad de transformación adaptada para transformar al menos una señal inicial derivada de la al menos una señal de referencia en al menos una señal de comparación mediante aplicación de la función de transformación;

- una unidad de comparación adaptada para efectuar una comparación de la señal biométrica transformada recibida con la al menos una señal de comparación; y

- una unidad de decisión adaptada para decidir si se autoriza un acceso basándose en la comparación efectuada por la unidad de comparación.

Un quinto aspecto de la presente invención propone un sistema de control de acceso que comprende:

- un sensor de señal biométrica según el tercer aspecto de la presente invención;
- un dispositivo de interfaz según el segundo aspecto de la presente invención; y
- un servidor de control de acceso según el cuarto aspecto de la presente invención.

Otros aspectos, objetivos y ventajas de la invención se irán poniendo de manifiesto con la lectura de la descripción de una de sus formas de realización.

La invención se comprenderá mejor asimismo con la ayuda de los dibujos, en los que:

la figura 1 ilustra una arquitectura de diferentes entidades comprendidas en un sistema de control de acceso según una forma de realización de la presente invención; y

la figura 2 ilustra una red de sensores en un sistema de control de acceso según una forma de realización de la presente invención.

En las siguientes secciones, se entiende por el término 'señal biométrica' una señal procedente de un sensor biométrico aplicado sobre una persona.

Tal señal biométrica puede corresponder a una imagen captada de una huella de la persona en cuestión, o también a una imagen captada de un iris, o una imagen del rostro o de una parte del rostro de esa persona.

Se entiende por el término 'señal de referencia' una señal biométrica de una persona para la que está autorizado el acceso controlado según una forma de realización de la presente invención. Una señal de referencia es proporcionada por un sensor biométrico, sin que se aplique una función de transformación en el sentido de la presente invención.

Se entiende por el término 'señal inicial derivada de una señal de referencia', bien sea directamente la señal de referencia, o bien incluso la señal de referencia previamente transformada mediante aplicación de una transformación inicial.

Una señal inicial es una señal de la que dispone el servidor. Esta puede, por ejemplo, estar almacenada en una base de datos gestionada por el servidor, o incluso ser proporcionada al servidor mediante cualquier medio de transmisión.

En las siguientes secciones, el parámetro común está sensiblemente sincronizado a nivel del dispositivo de interfaz y del servidor de control, de modo que el mismo parámetro se utiliza en el momento en que una señal biométrica captada es transformada a nivel del dispositivo de interfaz y en el momento en que la señal así transformada es recibida y procesada a nivel del servidor de control.

Una función de transformación no reversible en el sentido de la presente invención puede ser cualquier función no reversible que permite transformar o incluso deformar una imagen en una imagen deformada. Se puede utilizar en particular una de las funciones de transformación descritas en el documento US 6 836 554.

En el caso en que el sensor capta una imagen de huella, la función de transformación puede ser una función cuya aplicación consiste en una deformación de la imagen en el dominio espacial. Se puede descomponer así la imagen que ha de transformarse en una pluralidad de partes y seguidamente distribuir dichas partes de imagen así obtenidas en una distribución espacial diferente especificada.

En el presente caso, el parámetro común puede servir, por ejemplo, para especificar una nueva distribución de las partes de la imagen original. Este puede consistir asimismo en definir nuevas formas de las diferentes partes de la imagen que han de distribuirse según la distribución especificada. Se puede prever asimismo tomar en cuenta combinadamente los dos parámetros comunes apuntados más arriba.

En el caso en que el sensor capta una imagen del rostro o de una parte del rostro, la función de transformación también puede ser una función de deformación de la imagen captada en el dominio espacial. La imagen se puede descomponer, también en el presente caso, en una pluralidad de partes. Seguidamente se pueden modificar algunos contornos de esas partes así obtenidas, implicando así una deformación diferente de las diferentes partes para las que se han modificado los contornos.

En el presente caso, el parámetro común puede corresponder, por ejemplo, al número de partes que componen la imagen que ha de transformarse. Este puede corresponder asimismo a la modificación impuesta a al menos algunos de los contornos de algunas de las partes de la imagen que ha de transformarse.

En el caso en que el sensor capta una imagen del iris, la función de transformación puede ser asimismo una función de deformación de la imagen captada en el dominio espacial. Se puede descomponer, por ejemplo, una vista del iris en una pluralidad de sectores angulares. Seguidamente, la aplicación de la función de transformación puede consistir en modificar al menos algunos de los ángulos de esos sectores angulares así obtenidos, reduciendo algunos ángulos y aumentando algunos otros.

En el presente caso, el parámetro común puede ser utilizado para determinar un cambio en la reducción y/o en el aumento de algunos de esos ángulos.

Se puede prever parametrizar tal función de transformación mediante una pluralidad de parámetros comunes, según están definidos en la presente descripción.

La figura 1 ilustra una arquitectura de diferentes entidades comprendidas en un sistema de control de acceso según una forma de realización de la presente invención.

En las siguientes secciones, únicamente a título de ejemplo, la presente invención se describe en su aplicación a un control de acceso físico de personas en un sitio físico dado, mediante un control biométrico basado en características biométricas de huella. En tal contexto, se halla ubicado un sensor de señal biométrica según una forma de realización de la presente invención, por ejemplo, en una puerta de acceso a un edificio cuya entrada está controlada según una forma de realización de la presente invención. Así, en caso de estar autorizado el acceso, se puede prever la apertura de esa puerta.

Tal sistema de control de acceso comprende un servidor de control de acceso 12 que puede disponer de señales de comparación destinadas a ser comparadas con una señal transformada recibida que ha de controlarse. Comprende además un sensor de señal biométrica 11 y un dispositivo de interfaz 13.

En tal sistema de control de acceso, el sensor de señal biométrica 11 comprende una primera unidad de interfaz 111 adaptada para captar una imagen de una huella de una persona que pretende acceder al edificio protegido según una forma de realización de la presente invención. Este comprende además una segunda unidad de interfaz 112 adaptada para proporcionar al dispositivo de interfaz 13 una señal biométrica así captada.

El dispositivo de interfaz 13 comprende una unidad de gestión 133 adaptada para gestionar, por una parte, un parámetro común con el servidor de control, que toma valores diferentes con el paso del tiempo y, por otra parte, una primera función de transformación no reversible, siendo esta función parametrizada en función al menos del parámetro común. Comprende asimismo una primera unidad de interfaz 131 adaptada para recibir la señal biométrica captada desde el sensor. También comprende una unidad de transformación 135 adaptada para transformar la señal biométrica captada recibida por la primera unidad de interfaz en una señal biométrica transformada. Comprende además una segunda unidad de interfaz 132 adaptada para permitir la transmisión de la señal biométrica transformada por la unidad de transformación con destino al servidor de control 12.

Se puede prever que la segunda unidad de interfaz coopere con un dispositivo de transmisión 15 adaptado para realizar efectivamente la transmisión de la señal biométrica transformada con destino al servidor de control. Este dispositivo de transmisión 15 puede estar ubicado en el sensor o en el dispositivo de interfaz, o incluso separado del sensor 11 y del dispositivo de interfaz 13.

Un servidor de control 12 según una forma de realización de la presente invención puede comprender una unidad de gestión 123 adaptada para gestionar, por una parte, un parámetro, común con el dispositivo de interfaz 13, que toma valores diferentes con el paso del tiempo y, por otra parte, una segunda función de transformación no reversible, siendo esta función parametrizada en función al menos del parámetro común.

Este comprende asimismo una unidad de transformación 122 adaptada para transformar unas señales derivadas de las señales de referencia en respectivas señales de comparación mediante aplicación de la segunda función de transformación.

Este servidor 12 comprende además una unidad de interfaz 121 adaptada para recibir una señal biométrica transformada proporcionada por el dispositivo de interfaz 13. También comprende una unidad de comparación 124 adaptada para efectuar una comparación de la señal biométrica transformada recibida con las señales de comparación, así como una unidad de decisión 125 adaptada para decidir si se autoriza un acceso basándose en la comparación efectuada por la unidad de comparación 124.

En una forma de realización de la presente invención, el sensor 11 y el dispositivo de interfaz 13 son entidades diferentes de modo que, ventajosamente, el dispositivo de interfaz es amovible y móvil con independencia del sensor de señal biométrica 11. Así, se puede prever que cada persona que pretenda entrar en el edificio disponga de tal dispositivo de interfaz 13.

En una variante, el dispositivo de interfaz 13 puede estar comprendido en el sensor 11, de modo que las dos entidades se constituyan en una sola. En tal caso, se puede prever que el sensor y, con ello, el dispositivo de interfaz, esté fijo a nivel de la puerta de entrada del edificio cuyo acceso está protegido.

En este último caso, el sensor puede estar adaptado para recibir el parámetro común de la persona que se está controlando a través de cualquier interfaz de registro. Seguidamente, este parámetro se utiliza a nivel del dispositivo de interfaz al objeto de parametrizar la primera función de transformación.

A continuación, este parámetro es enviado entonces al servidor, de modo que éste pueda parametrizar también la segunda función de transformación. Así, el parámetro común, en primer lugar, es registrado por la persona que pretende acceder al edificio y seguidamente es enviado al servidor de control. Al proceder de esta manera, las respectivas funciones de transformación se pueden parametrizar correctamente al objeto de, por una parte, proporcionar una señal biométrica captada transformada mediante la primera función de transformación parametrizada mediante el parámetro común a nivel del sensor y, por otra parte, de obtener señales de comparación correspondientes a las señales de referencia transformadas mediante la aplicación de una función de transformación equivalente a la primera función de transformación.

Se puede prever que el servidor de control 12 disponga directamente de las señales de referencia. En tal caso, la aplicación de la primera función de transformación puede equivaler directamente a la aplicación de la segunda función de transformación.

En una variante, el servidor de control puede disponer de señales iniciales que se derivan de las señales de referencia, correspondiendo estas señales iniciales a las señales de referencia previamente transformadas mediante la aplicación de una función de transformación inicial. En tal caso, se puede prever que la aplicación de la primera función de transformación equivale a la aplicación combinada de la segunda función y de la función de transformación inicial.

Estas señales iniciales pueden estar a disposición del servidor 12, por ejemplo mediante una base de datos en la que están almacenadas y a la que el servidor tiene acceso, o incluso mediante cualquier otro medio.

En una forma de realización de la presente invención, una persona dispone por tanto de un dispositivo de interfaz 13, que ésta conecta a un sensor de señal biométrica 11 situado cerca de la puerta que la persona pretende franquear. Seguidamente, coloca por ejemplo su índice sobre el sensor 11. El sensor 11 captura una imagen de la huella del índice de esa persona. Seguidamente, ese sensor 11 proporciona esa imagen biométrica al dispositivo de interfaz 13 conectado, en forma de una señal biométrica. Esa señal biométrica es recibida a nivel de la primera unidad de interfaz 131 del dispositivo de interfaz 13.

A continuación, es proporcionada a la unidad de transformación 135. Esta última transforma esa señal biométrica captada mediante aplicación de la primera función de transformación, parametrizada con el valor del parámetro común, proporcionado por la unidad de gestión 133. El valor de este parámetro común evoluciona con el tiempo de manera sensiblemente síncrona a nivel de la unidad de gestión 133 del dispositivo de interfaz 13 y a nivel de la unidad de gestión 123 del servidor de control 12.

Se obtiene así una señal biométrica transformada, que se transmite a nivel de la segunda unidad de interfaz 132. Esta unidad de interfaz está adaptada para cooperar con un dispositivo de transmisión 15 que puede estar ya sea ubicado conjuntamente con esta segunda unidad de interfaz, o bien ser una entidad separada del dispositivo de interfaz.

Seguidamente, esa señal biométrica transformada 14 se transmite al servidor de control 12. Con objeto de procesar esa señal biométrica transformada, el servidor de control 12 obtiene señales de referencia transformadas según una función de transformación similar a la que se ha aplicado a nivel del dispositivo de interfaz 13.

A tal efecto, se puede prever que el servidor almacena, o cuando menos tiene acceso a las señales de referencia de las personas autorizadas y que dispone de la misma función de transformación que la que está gestionada por la unidad de gestión del dispositivo de interfaz 13. En tal caso, aquel aplica a las señales de referencia esa función de transformación parametrizada con el parámetro común. Consecuencia de ello son unas señales de comparación correspondientes a las señales de referencia transformadas de la misma manera que, en el lado del usuario, se ha transformado la señal biométrica captada que ha de controlarse.

Así, el servidor compara la señal transformada recibida y las señales de comparación más arriba descritas, por donde deduce si la persona que se está controlando forma parte o no de las personas autorizadas. Esta comparación encaminada a comparar dos imágenes captadas potencialmente de diferente manera, y luego transformadas, no es una comparación estricta.

En otra variante, el servidor de control 12 sólo dispone de señales de referencia en una forma previamente transformada, correspondientes a la aplicación de una función de transformación inicial sobre las señales de referencia no reversible. Así, se incrementa la protección puesto que, aunque un atacante pueda recuperar una de las señales de las que dispone el servidor de control, no tiene acceso a la señal de referencia original.

En esta variante, la unidad de gestión 123 del servidor de control 12 gestiona una segunda función de transformación que difiere de la primera función del dispositivo de interfaz 13. En efecto, más concretamente, la

primera función de transformación equivale a una combinación de la segunda función de transformación y de la función de transformación inicial. No obstante, la primera y la segunda función de transformación se parametrizan, también en el presente caso, de igual manera mediante el parámetro común.

En una forma de realización de la presente invención, el sistema de control de acceso está basado además en un identificador de la persona que ha de controlarse. Tal variante permite mejorar las prestaciones de procesamiento de señal a nivel del servidor de control 12.

En efecto, en tal caso, el servidor de control gestiona una asociación de las señales de comparación con los respectivos identificadores de las personas autorizadas en el sistema de control. Seguidamente, la persona que se está controlando proporciona su identificador al servidor por intermedio, por ejemplo, del dispositivo de interfaz, o incluso por cualquier otra interfaz que se ofrezca a la persona a nivel de la puerta de entrada controlada. Así, en tales condiciones, el servidor de control está en disposición de recuperar la señal de comparación asociada al identificador recibido, sin tener que comparar la señal biométrica captada transformada recibida con una pluralidad de señales de comparación.

La figura 2 ilustra una red de sensores en un sistema de control de acceso según una forma de realización de la presente invención. Así, en este contexto, cada uno de los sensores del sistema puede hallarse posicionado en diferentes puertas de entrada de un sitio físico o incluso, entre estos sensores, algunos pueden hallarse ubicados conjuntamente con estaciones informáticas para realizar un control de acceso a datos informáticos, por ejemplo.

Dos de ellos están realizando un control de acceso y a ellos están conectados unos dispositivos de interfaz 13.

Se puede prever que se utilicen funciones de transformación no reversibles diferentes en función de las aplicaciones controladas.

En un sistema de control según una forma de realización de la presente invención, en función del parámetro común, se está en disposición de modificar la transformación de las señales biométricas manipuladas en el transcurso de los sucesivos controles de acceso para una misma persona, al objeto de mejorar la fiabilidad de los controles. En efecto, en función del nivel de fiabilidad que se persigue, se puede definir una evolución más o menos rápida del parámetro común.

Ventajosamente, se puede incluso definir fácilmente una variación del parámetro común con cada uno de los controles ejecutados para misma persona, al objeto de garantizar una protección completa contra los ataques basados en la nueva reproducción de una señal biométrica transformada interceptada.

REIVINDICACIONES

1. Procedimiento de control de acceso en un sistema de control de acceso (10) que comprende:

un servidor de control de acceso (12) adaptado para controlar un acceso;

al menos un sensor de señal biométrica (11); y

un dispositivo de interfaz (13) adaptado para estar relacionado, por una parte, con el servidor de control y, por otra parte, con el sensor;

autorizándose dicho acceso a al menos una persona que tiene asociada una señal de referencia que comprende información biométrica correspondiente;

gestionando el servidor de control y el dispositivo de interfaz, por una parte, un parámetro común que toma valores diferentes con el paso del tiempo y, por otra parte, respectivamente una primera y una segunda función de transformación no reversible, siendo dichas funciones de transformación primera y segunda parametrizadas en función al menos de dicho parámetro común;

comprendiendo dicho procedimiento las siguientes etapas:

/a/ a nivel del sensor, captar una señal biométrica y proporcionar dicha señal biométrica captada al dispositivo de interfaz;

/b/ a nivel del dispositivo de interfaz, obtener una señal biométrica transformada aplicando la primera función de transformación a un elemento de entre un grupo que comprende al menos una característica derivada de dicha señal biométrica captada y dicha señal biométrica captada; y transmitir (14) dicha señal biométrica transformada con destino al servidor de control;

/c/ a nivel del servidor de control, efectuar una comparación de la señal biométrica transformada con al menos una señal de comparación, correspondiendo dicha señal de comparación a una señal resultante de la aplicación de la segunda función de transformación a una señal inicial derivada de la señal de referencia; y

/d/ basándose en dicha comparación, decidir si se autoriza un acceso.

2. Procedimiento de control de acceso según la reivindicación 1, en el que los valores del parámetro común son función de los valores de un contador, gestionado a nivel del dispositivo de interfaz y del servidor, del número de señales biométricas transformadas que son transmitidas y recibidas respectivamente por el dispositivo de interfaz y el servidor.

3. Procedimiento de control de acceso según una cualquiera de las anteriores reivindicaciones, en el que, al estar sincronizados el servidor de control de acceso y el dispositivo de interfaz en una referencia temporal común, los valores del parámetro común son función del valor de la referencia temporal común.

4. Procedimiento de control de acceso según una cualquiera de las anteriores reivindicaciones, en el que los valores del parámetro común se registran a nivel del dispositivo de interfaz y en el que cada nuevo valor del parámetro común se transmite al servidor de control.

5. Procedimiento de control de acceso según una cualquiera de las anteriores reivindicaciones, en el que el sistema de control de acceso controla el acceso a una pluralidad de tipos de aplicaciones y en el que con dicha pluralidad de tipos de aplicaciones se asocia respectivamente una pluralidad de pares de una primera función de transformación no reversible a nivel del dispositivo de interfaz y de una segunda función de transformación no reversible a nivel del servidor de control.

6. Procedimiento de control de acceso según una cualquiera de las anteriores reivindicaciones, en el que la señal inicial comprende la señal de referencia y en el que la aplicación de la primera y la aplicación de la segunda función de transformación parametrizadas no reversibles son equivalentes.

7. Procedimiento de control de acceso según una cualquiera de las anteriores reivindicaciones, en el que la señal inicial derivada de la señal de referencia, correspondiente a la al menos una persona autorizada, se obtiene mediante aplicación de una función de transformación inicial no reversible a la señal de referencia; y en el que la primera función de transformación equivale a una combinación de la segunda función de transformación y de dicha función de transformación inicial.

8. Procedimiento de control de acceso según una cualquiera de las anteriores reivindicaciones, en el que se asocia un identificador con el dispositivo de interfaz y/o con la al menos una persona a la que se autoriza el acceso y en el que el servidor de control gestiona una asociación de la al menos una señal de comparación con dicho identificador;

comprendiendo además dicho procedimiento, antes de la etapa /c/, las siguientes etapas:

- obtener, a nivel del dispositivo de interfaz, un identificador correspondiente a la señal biométrica captada;

- transmitir al servidor de control dicho identificador; y

- a nivel del servidor de control, recuperar la señal de comparación asociada a dicho identificador recibido.

9. Dispositivo de interfaz (13) en un sistema de control de acceso (10) que comprende además, por una parte, un servidor de control de acceso (12) adaptado para controlar un acceso; y, por otra parte, al menos un sensor de señal biométrica (11);

autorizándose dicho acceso a al menos una persona que tiene asociada una señal de referencia que comprende información biométrica correspondiente;

comprendiendo dicho dispositivo de interfaz:

- una unidad de gestión (133) adaptada para gestionar, por una parte, un parámetro, común con el servidor de control, que toma valores diferentes con el paso del tiempo y, por otra parte, una función de transformación no reversible, siendo dicha función de transformación parametrizada en función de al menos dicho parámetro común;

- una primera unidad de interfaz (131) adaptada para recibir una señal biométrica captada desde el sensor;

- una unidad de transformación (135) adaptada para transformar una señal biométrica captada en una señal biométrica transformada aplicando la función de transformación a un elemento de entre un grupo que comprende al menos una característica derivada de dicha señal biométrica captada y dicha señal biométrica captada; y

- una segunda unidad de interfaz (132) adaptada para cooperar con un dispositivo de transmisión (15) adaptado para transmitir una señal biométrica transformada por la unidad de transformación con destino al servidor de control.

10. Dispositivo de interfaz (13) según la reivindicación 9, en el que los valores del parámetro común son función de los valores de un contador, gestionado por la unidad de gestión (133), del número de señales biométricas transformadas que se envían respectivamente al servidor.

11. Dispositivo de interfaz (13) según la reivindicación 9 ó 10, en el que, al estar sincronizados el servidor de control de acceso y el dispositivo de interfaz en una referencia temporal común, los valores del parámetro común son función del valor de la referencia temporal común.

12. Dispositivo de interfaz (13) según una cualquiera de las reivindicaciones 9 a 11, en el que los valores del parámetro común se registran a nivel del dispositivo de interfaz y en el que cada nuevo valor del parámetro común se transmite al servidor de control.

13. Sensor de señal biométrica (11) que comprende un dispositivo de interfaz según una cualquiera de las reivindicaciones 9 a 12.

14. Servidor de control de acceso (12) en un sistema de control de acceso (10) que comprende además al menos un sensor de señal biométrica (11); y un dispositivo de interfaz (13) adaptado para estar relacionado, por una parte, con el servidor de control y, por otra parte, con el sensor;

autorizándose dicho acceso a al menos una persona que tiene asociada una señal de referencia que comprende información biométrica correspondiente; comprendiendo dicho servidor de control:

- una unidad de interfaz (121) adaptada para recibir una señal biométrica transformada proporcionada por dicho dispositivo de interfaz (13);

- una unidad de gestión (123) adaptada para gestionar, por una parte, un parámetro, común con el dispositivo de interfaz, que toma valores diferentes con el paso del tiempo y, por otra parte, una función de transformación no reversible, siendo dicha función de transformación parametrizada en función de al menos dicho parámetro común;

- una unidad de transformación (122) adaptada para transformar al menos una señal inicial derivada de la al menos una señal de referencia en al menos una señal de comparación mediante aplicación de la función de transformación a dicha señal inicial;

- una unidad de comparación (124) adaptada para efectuar una comparación de la señal biométrica transformada recibida con la al menos una señal de comparación; y

- una unidad de decisión (125) adaptada para decidir si se autoriza un acceso basándose en la comparación

efectuada por la unidad de comparación.

15. Sistema de control de acceso que comprende:

- un sensor de señal biométrica según la reivindicación 13;
- un dispositivo de interfaz (13) según una cualquiera de las reivindicaciones 9 a 12; y
- un servidor de control de acceso (12) según la reivindicación 14.

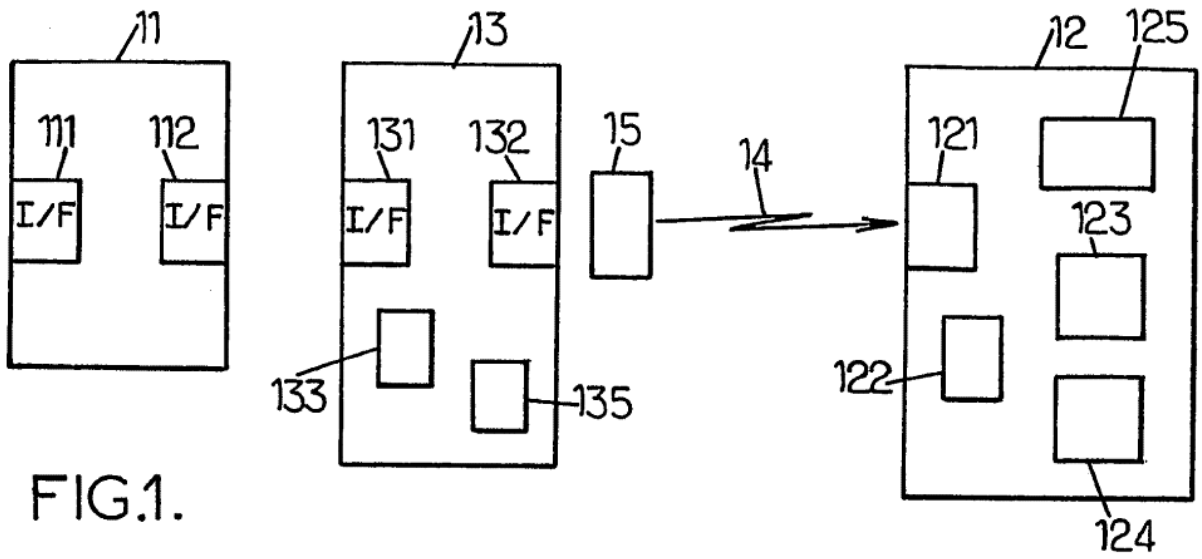
11
111
112
I/F
I/F
13
131
132
I/F
I/F
15
14
133
135
12
125
121
123
122
124

FIG.1.

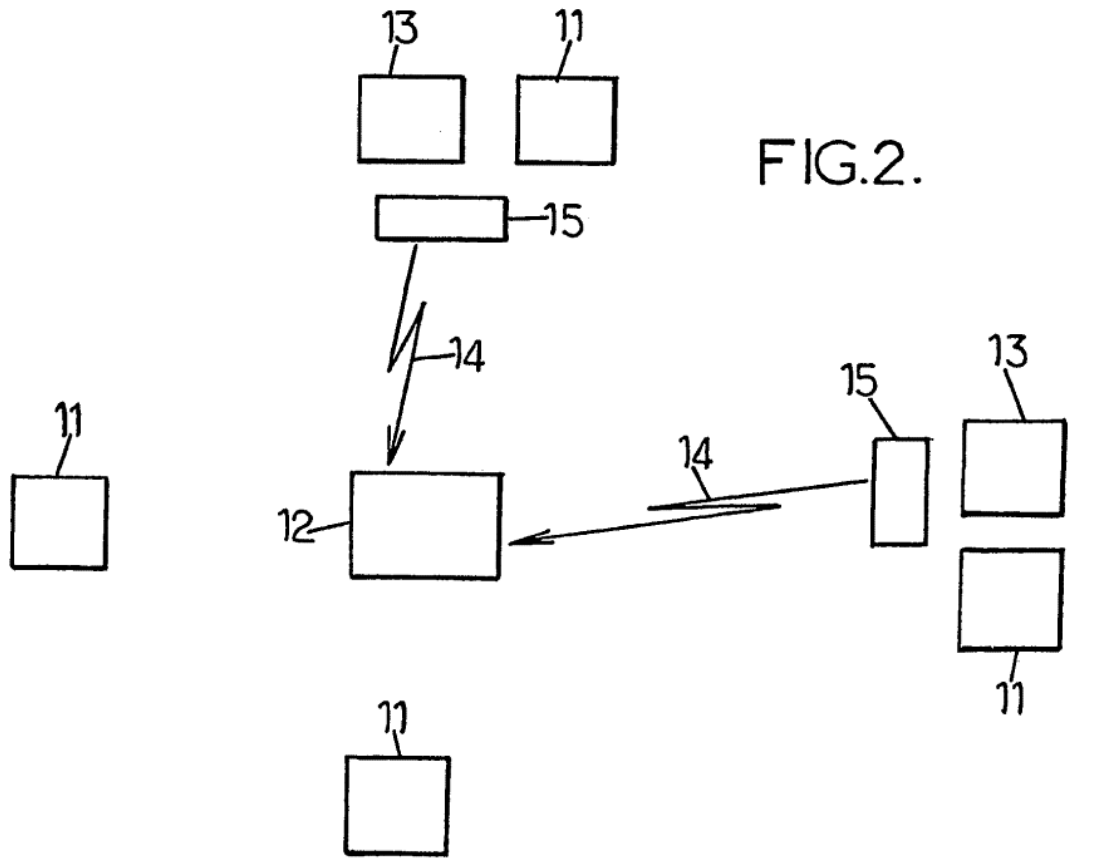
13
11
15
14
11
12
15
13
14
11
11

FIG.2.