ETSIT UPM

Isdefe

Cuadernos
Cátedra
ISDEFE-UPM

3

Biometría y Seguridad

Javier Ortega García
Fernando Alonso Fernández
Rafael Coomonte Belmonte

Biometría y Seguridad

Autores:
Javier Ortega García
Fernando Alonso Fernández
Grupo de Reconocimiento Biométrico-ATVS
Universidad Autónoma de Madrid

Con la colaboración y revisión de:
Rafael Coomonte Belmonte
Cátedra ISDEFE-UPM
E.T.S.I. Telecomunicación

Primera edición: Mayo 2008

Edita:
Fundación Rogelio Segovia para el
Desarrollo de las Telecomunicaciones
Ciudad Universitaria, s/n
28040-Madrid

Imprime:
E.T.S.I. de Telecomunicación
Universidad Politécnica de Madrid
Ciudad Universitaria, s/n
28040-Madrid
Diseño de cubierta y
maquetación: Rocio Ortega

ISBN (13): 978-84-7402-350-3
ISBN (10): 84-7402-350-5
Depósito Legal: M-23567-2008

Índice

Presentación

Con este tercer "Cuaderno de la Cátedra Isdefe" se inicia una serie dedicada a ofrecer unas monografías sobre tecnologías importantes para el área de la Seguridad. Con rigor académico y exposición clara se muestra en este número una visión panorámica de los sistemas biométricos con las diversas tecnologías y aplicaciones y las tendencias futuras de desarrollo.

El cuaderno contiene también un catálogo, no exhaustivo, de empresas y grupos de I+D con actividades en el área de la Biometría, así como las políticas de desarrollo.

Espero que el lector pueda tener una visión de conjunto de lo que es, para lo que sirve y cómo y quiénes están involucrados en el área de las aplicaciones de la Biometría a la Seguridad.

Miguel Ángel Panduro
Consejero Delegado de Isdefe

Luis Martínez Míguez
Director de tecnología ISDEFE

Capítulo 1

Aspectos generales

1. Aspectos generales

1.1. El reconocimiento biométrico

Desde la antigüedad los seres humanos han utilizado los rasgos biométricos tales como la cara y la voz para reconocerse unos a otros [45]. Actualmente en una sociedad interconectada como la nuestra, establecer de forma unívoca la identidad de un individuo se ha convertido en un aspecto critico, y a la vez cotidiano, en una gran variedad de escenarios que se extienden desde el uso de cajeros automáticos hasta el permiso de entrada a un país. El reconocimiento biométrico, definido como la técnica que posibilita la identificación automática de individuos basándose en sus características físicas o de comportamiento, está ganando gran aceptación como método para determinar la identidad de cada persona y ya se está utilizando en multitud de aplicaciones tanto comerciales como público-gubernamentales, en ámbitos tanto civiles como forenses (es decir, relacionadas con lo policial y lo legal). Mediante el uso del reconocimiento biométrico, es posible establecer la identidad de una persona mediante "algo que se es", a diferencia de los tradicionales sistemas basados en "algo que se posee" (como un DNI, una tarjeta de identificación o una llave), que puede perderse o robarse, o en "algo que se sabe" (como una clave), que puede ser olvidado [58].

Orígenes y evolución

La primera referencia que se tiene acerca del uso de una característica biométrica para identificar individuos [14, 75] se remonta al siglo VIII en China, mediante el uso de huellas dactilares en documentos y en esculturas de arcilla. En el año 1000 DC. Quintiliano usó las huellas dejadas por las palmas de unas manos ensangrentadas para esclarecer un crimen y siglos más tarde, en 1686, Marcelo Malpigio hizo el primer estudio sistemático de huellas dactilares.

Alphonse Bertillon, jefe de la sección de delitos criminales de la región de París, puso en práctica a mitad del siglo XIX la idea de utilizar rasgos corporales para identificar criminales. A finales de dicho siglo, se estableció la idea de que las huellas dactilares eran lo suficientemente distintivas para identificar personas, hecho que condujo a muchos departamentos de policía a almacenar las huellas de criminales con el fin de cotejarlas con huellas aparecidas en la escena de un crimen.

En 1941, en los Laboratorios Bell de Murray Hill (Nueva Jersey), comenzó el estudio de la identificación por voz. En 1986, sir Alec Jeffreys utilizó por primera vez el ADN para identificar al autor de unos asesinatos en Inglaterra.

El uso del reconocimiento biométrico como tecnología comercial tiene su inicio en los años 70 con los primeros sistemas automáticos de huellas dactilares. A partir de los años 90, con el desarrollo y crecimiento de la informática y la microelectrónica, el interés por el reconocimiento biométrico ha crecido de manera exponencial. Aunque comenzó a usarse en entornos exclusivamente policiales y forenses, es cada vez mayor el número de aplicaciones civiles y dispositivos personales que utilizan el reconocimiento biométrico como método de identificación personal.

Características de los rasgos biométricos

En función de las características usadas para la identificación personal, se establecen dos grandes tipos de rasgos biométricos, dependiendo de si se fijan en los aspectos físicos del individuo o si se fijan en aspectos vinculados a la conducta [44]. Entre los rasgos vinculados a los aspectos físicos podemos encontrar, por ejemplo, la huella dactilar, el iris, la geometría de la mano, la cara, etc. Por otro lado, ejemplos de rasgos vinculados a los aspectos de la conducta son la escritura manuscrita, la firma, la voz, la dinámica de tecleo o la forma de andar. La característica principal de los rasgos conductuales es que el individuo tiene que hacer una "realización" de los mismos (Ej. firmar o hablar), a diferencia de los rasgos físicos, que siempre se encuentran presentes.

Pero, ¿qué propiedades debe cumplir un rasgo para poder ser considerado como identificativo? Cualquier característica, física o de conducta, puede usarse como característica biométrica en tanto que cumpla las siguientes propiedades:

- *Universalidad*: todo el mundo debe poseer esa característica.
- *Unicidad*: dos personas cualesquiera deben ser suficientemente diferentes en términos de ese rasgo, es decir, un mismo rasgo para dos personas diferentes nunca puede ser idéntico.
- *Permanencia*: el rasgo debe permanecer suficientemente invariable en el tiempo durante un periodo de tiempo aceptable.
- *Evaluabilidad*: el rasgo debe poder ser medido cuantitativamente.

Aparte de estas propiedades, desde el punto de vista práctico de un sistema de reconocimiento, hay otro conjunto de propiedades que deben satisfacerse:

- *Rendimiento*: hace referencia al error cometido en el reconocimiento de individuos, a la velocidad y recursos necesarios para llevarlo a cabo,

así como a los factores externos que afecten a las capacidades de reconocimiento del sistema.

- *Aceptabilidad*: los usuarios deben estar dispuestos a emplear ese rasgo en las actividades de su vida cotidiana.

- *Fraude*: los sistemas que usen ese rasgo deben ser suficientemente seguros de forma que resulte difícil atacarlos.

En resumen, un sistema práctico que haga uso del reconocimiento biométrico debe cumplir con los requisitos de precisión, velocidad y utilización de recursos, debe ser aceptado por la población a la que se dirige y debe ser lo suficientemente robusto a los intentos de fraude y ataques a los que pueda ser sometido. Cada rasgo biométrico tiene sus ventajas y sus inconvenientes, y no hay ningún rasgo que cumpla con alguna de las propiedades anteriores al 100% o que cumpla con todas a la vez de forma satisfactoria, por lo que ninguno de ellos puede cubrir de forma efectiva las necesidades de todas las aplicaciones y siempre será necesario algún tipo de compromiso. En el Capítulo 3 podemos encontrar una descripción detallada de los rasgos más utilizados, junto a sus ventajas e inconvenientes.

1.2. Ventajas del reconocimiento biométrico sobre las técnicas tradicionales de autenticación

La autenticación personal no es un problema reciente, sino que la sociedad hace décadas que ha adoptado ampliamente mecanismos para reconocer individuos. Los métodos clásicos de autenticación más usados son:

- Mecanismos basados en posesión física de elementos o "tokens" tales como llaves, pasaportes, tarjetas magnéticas, etc.

- Mecanismos basados en el *conocimiento* de información secreta conocida solamente por las personas adecuadas, como claves personales o números PIN. También puede incluirse información que quizá no sea secreta, como un nombre de usuario.

Estas técnicas se usan actualmente en un amplio abanico de aplicaciones, pero tienen una serie de inconvenientes que ponen en entredicho su utilidad en aplicaciones "sensibles" como acceso a datos bancarios online, acceso a datos médicos confidenciales, pagos con tarjeta de crédito, etc. El reconocimiento biométrico es capaz de proporcionar un mayor grado de seguridad que estos métodos tradicionales, de tal manera que los recursos sean accesibles solamente por usuarios autorizados. Las claves y PINs pueden copiarse u olvidarse, mientras que los "tokens" pueden robarse.

Por el contrario, los datos biométricos no pueden copiarse, robarse u olvidarse.

Muchos usuarios eligen como clave o PIN palabras o números sencillos, de tal manera que no es muy complicado adivinarlos o "romperlos". Una encuesta realizada en el año 2001 a 1200 trabajadores británicos [45] dio como resultado que casi la mitad elegían su propio nombre, el nombre de una mascota o el de un familiar como clave de acceso, mientras que otros elegían para sus claves nombres como "Homer Simpson" o "Darth Vader". Aunque es recomendable usar distintas claves para distintos servicios y cambiarlas cada cierto tiempo, el creciente número de aplicaciones hacen que la mayoría de la gente use la misma clave para todo y sin cambiarla nunca. Si una de nuestras claves se ve comprometida en una aplicación, es muy probable que ello suponga un peligro para el resto de aplicaciones. Por ejemplo, un atacante podría crear una página Web falsa con un reclamo tal como regalar saldo para el teléfono móvil si el usuario se registra con un nombre y una clave. A continuación, el atacante podría utilizar el nombre y la clave para intentar acceder a otros servicios donde el usuario esté registrado (correo electrónico, cuentas bancarias online, etc.) y es muy probable que tuviera éxito. Otro tipo posible de ataque es el de "fuerza bruta", donde un sistema informático genera gran cantidad de contraseñas automáticamente probando combinaciones de letras y números según algún tipo de lógica (por ejemplo, escogiendo las palabras más usadas de un idioma a partir de un diccionario). Cuando más sencilla sea la clave, mayores posibilidades hay de que el ataque tenga éxito.

Otra opción es forzar el uso de claves largas y complejas, que combinen números y letras, como por ejemplo "B12s3CuR4m". Pero a cambio, son más difíciles de recordar, lo que lleva a que los usuarios la tengan escrita en algún lugar fácilmente accesible, como un "post-it" o una libreta en algún lugar del escritorio. Basta que un atacante "rompa" solamente la clave de un empleado para obtener acceso a la red de la empresa, por lo que una clave "fácil de obtener" compromete la seguridad de todo un sistema. En estos casos se dice que un sistema es tanto más seguro cuanto más difícil sean de obtener cualquiera de sus claves. Una clave fácilmente averiguable supone un punto débil en el sistema. Con el reconocimiento biométrico, todos los usuarios tienen relativamente el mismo nivel de seguridad y no existe en principio una clave mucho más fácil de romper que otras. Igualmente, el reconocimiento biométrico ofrece mayor comodidad para el usuario, ya que no es necesario recordar múltiples claves complejas ni es necesario cambiarlas cada cierto tiempo.

Las claves igualmente suelen compartirse entre grupos de personas, bien por sencillez (por ejemplo, entre los administradores de una red informá-

tica) o por cortesía (cuando le presto la clave de mi cuenta a un compañero de trabajo). Esto supone que no hay manera de saber quién está realmente accediendo al sistema en cada momento, o incluso si la persona que está haciendo uso de la clave está autorizada para ello. Lo mismo sucede con los "tokens", por ejemplo cuando se utilizan varias copias de la llave que permite acceder a una instalación y llega un punto que se pierde el control de quién tiene copia y quién no, con el riesgo añadido de que puede perderse alguna de las copias. Por el contrario, los datos biométricos no pueden compartirse de esta manera ni perderse, siendo necesario que la persona a ser reconocida esté físicamente presente en el punto de acceso.

Otra de las ventajas del reconocimiento biométrico estriba en que permite determinar si una persona ha sido registrada más de una vez en un sistema (por ejemplo, si un individuo posee varios DNIs o carnés de conducir bajo diferentes identidades). Averiguar esto con otros mecanismos distintos del reconocimiento biométrico resulta bastante complicado, cuando no imposible. Esto es válido no solamente para detectar el fraude, sino para prevenirlo, ya que la presencia de un sistema biométrico puede ser suficiente para disuadir a un individuo de intentar registrarse varias veces.

Una ventaja evidente del reconocimiento biométrico es su uso en modo vigilancia, como se describe más adelante en la Sección 2.1, especialmente en aplicaciones forenses o de seguridad pública. Supongamos por ejemplo que tenemos una lista con los 100 terroristas internacionales más buscados. Verificar dicha lista contra todas las personas que transitan a diario por un gran aeropuerto (unas 200.000) supone un gran coste en personal de seguridad y suele traducirse en incomodidad para el usuario, que tiene que soportar enormes colas de espera. Un sistema biométrico supone en este caso un ahorro considerable en personal de seguridad así como mayor agilidad en el trámite. Por otro lado, el personal de seguridad está sujeto a la fatiga y al tedio de una tarea repetitiva -verificar sujetos frente a una lista de criminales -, factores que no afectan a un sistema biométrico. Un ejemplo similar es la búsqueda de huellas obtenidas en la escena de un crimen en una base de datos de criminales. En este caso, podemos hablar de cientos de miles (incluso de millones) de identidades entre las que buscar.

No obstante, a pesar de las claras ventajas del reconocimiento biométrico, hay que decir que no es la panacea. Como iremos viendo a lo largo de esta contribución, el reconocimiento biométrico no es la solución en todos los casos y situaciones. A la hora de diseñar un sistema que haga uso del reconocimiento biométrico, hay que preguntarse si el entorno donde va a usarse es el adecuado y si el beneficio que proporciona compensa los costes

y riesgos. En cualquier caso, debemos considerar que en combinación con métodos de autenticación por posesión y/o conocimiento, el reconocimiento biométrico permite obtener potentes herramientas para la identificación personal.

Capítulo 2

Sistemas automáticos de reconocimiento

2. Sistemas automáticos de reconocimiento

2.1. Estructura general de un sistema biométrico

Un sistema biométrico esencialmente es un reconocedor de patrones que captura datos biométricos de un individuo, extrae un conjunto de características a partir de dichos datos y las compara con otros patrones previamente almacenados en el sistema [78]. Todos los sistemas de reconocimiento de patrones poseen una estructura funcional común formada por varias fases cuya forma de proceder depende de la naturaleza del patrón o señal a reconocer. La Figura 1 muestra esta estructura. En general el usuario únicamente tiene acceso al sensor, el cual captura el rasgo biométrico. A continuación se describen brevemente cada una de estas etapas.

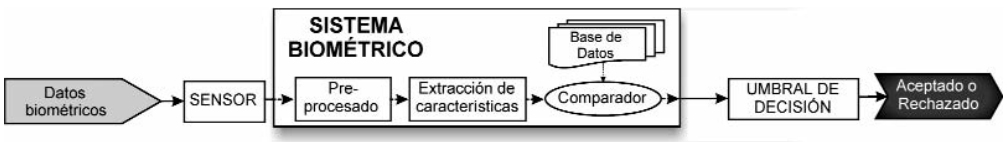


Figura 1. Arquitectura de un sistema de reconocimiento biométrico.

Adquisición de datos: En esta fase se recogen los datos analógicos de partida a través de un sensor y se convierten a un formato digital. Este proceso es determinante ya que de él depende la cantidad y la calidad de la información adquirida, la implementación de las siguientes fases, y, por tanto, el resultado final que se obtiene.

Preprocesado: En algunos casos es necesario acondicionar la información capturada para eliminar posibles ruidos o distorsiones producidas en la etapa de adquisición, o para normalizar la información a unos rangos específicos para tener una mayor efectividad en el reconocimiento posterior.

Extracción de características: En esta etapa se elimina la información que no resulte útil en el proceso de reconocimiento, bien por no ser específica de cada individuo o por ser redundante. De este modo, se extraen únicamente aquellas características que sean discriminantes entre distintos individuos y que al mismo tiempo permanezcan invariables

para un mismo usuario, reduciéndose así mismo la duración de todo el proceso de reconocimiento y su coste computacional.

Generación de un modelo y comparación de patrones: Una vez extraídas las características más significativas, se elabora un modelo que representa a cada individuo. Dichos modelos se almacenan en la base de datos del sistema y permiten, en la etapa operativa del sistema de reconocimiento, la comparación entre los datos que se capturen y el modelo de un individuo en particular.

Base de datos: Es donde se almacenan los modelos que representan la identidad de cada usuario del sistema. Dependiendo del tipo de aplicación, los datos usados para generar el modelo de un usuario pueden capturarse bajo supervisión de un operador o no. De la misma manera, la base de datos puede estar almacenada en un lugar único centralizado o cada usuario puede llevar una tarjeta inteligente que almacene únicamente el modelo de su identidad. Asimismo, es usual que con el paso del tiempo, los modelos de cada usuario se actualicen para tomar en consideración posibles variaciones del rasgo biométrico en cuestión.

Umbral de decisión: La comparación entre los datos de entrada y un modelo de identidad extraído de la base de datos está regulada por un umbral. Si la comparación supera cierto umbral de similitud, se indica que los datos de entrada y el modelo corresponden al mismo individuo y en caso contrario, no.

2.2. Modos de operación de un sistema biométrico

Los sistemas automáticos de reconocimiento de patrones pueden trabajar en tres modos de operación distintos: registro, identificación y verificación (se contempla también un modo vigilancia, que es un caso particular del modo identificación). En el modo de registro se genera la base de datos con la que se compararán los datos de entrada. La forma en que se realiza dicha comparación da lugar a los otros dos modos de funcionamiento: modo identificación y modo verificación.

Modo registro o "enrollment": este modo de operación consiste en añadir patrones o modelos a la base de datos manejada por el sistema (Figura 2). Los usuarios son dados de alta en el sistema y para ello se realiza la adquisición de sus rasgos biométricos, se extraen sus características y se genera un modelo o patrón representativo del individuo correspondiente, que queda almacenado en la base de datos de usuarios del sistema. No se realiza por tanto comparación alguna en este modo de trabajo. En la base de datos se pueden almacenar también

otros datos personales de los usuarios (nombre, apellidos, fecha de nacimiento, etc.).

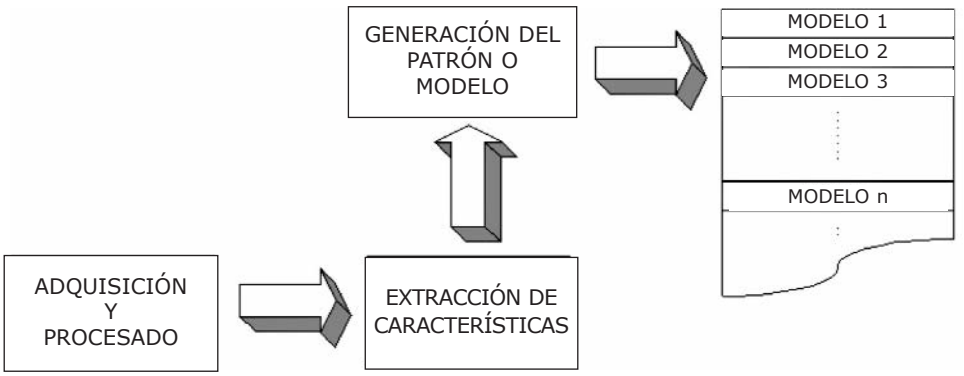


Figura 2. Operación en Modo Registro.

Modo verificación (¿es esta persona quien dice ser?): en este modo, es necesario proporcionar los datos de entrada y el modelo al que supuestamente pertenece dicha información (una "identidad pretendida"). El sistema valida la identidad del individuo comparando ambos (Figura 3). Si la comparación supera cierto umbral de similitud, se indica que los datos capturados corresponden a la identidad pretendida y en caso contrario, que se trata de un impostor. La identidad pretendida normalmente se indica a través de un número PIN o un nombre de usuario, y el sistema efectúa una comparación "uno-a-uno" para determinar si dicha identidad pretendida es correcta o no. El modo verificación se usa para lo que se conoce como "reconocimiento positivo", donde el objetivo es evitar que múltiples personas utilicen la misma identidad. Los sistemas que funcionan en este modo pretenden ser amigables para el usuario, por ejemplo en aplicaciones como pago con tarjeta de crédito, acceso físico a instalaciones, enseñanza a distancia, uso de teléfonos móviles u ordenadores, etc.

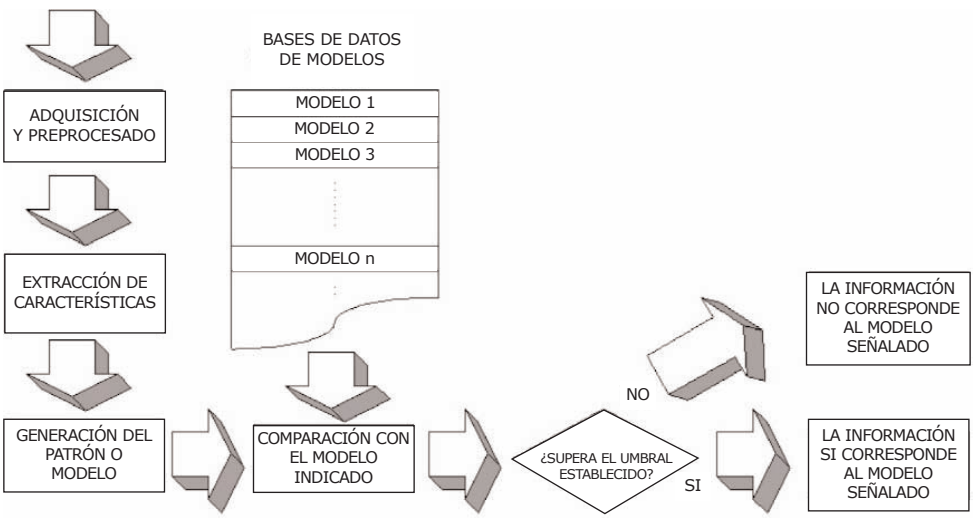


Figura 3. Operación en Modo Verificación.

Modo identificación (¿quién es esta persona?): en este modo de trabajo, únicamente se introducen los datos a autenticar, a partir de los cuales el sistema debe decidir qué identidad de la base de datos corresponde con la información adquirida (Figura 4). Para ello, el sistema compara los datos capturados con todos los patrones almacenados en el sistema (típicamente millones, por lo que este modo de funcionamiento requiere una gran capacidad de procesamiento). En este caso, se efectúa una comparación "uno-a-muchos", sin que el usuario tenga que solicitar

ninguna identidad pretendida. En este tipo de funcionamiento, el sistema puede devolver dos posibles resultados:

- La identidad de la base de datos que obtuvo mayor semejanza en la comparación.
- Ninguna identidad de la base de datos se corresponde con los datos adquiridos.

Dependiendo del resultado ofrecido por el sistema, se pueden diferenciar dos grandes grupos:

- Sistemas de identificación en conjunto cerrado (closed set): sólo ofrecen el primer resultado.
- Sistemas de identificación en conjunto abierto (open set): son los que contemplan ambas posibilidades.

En este último caso, para determinar si la información corresponde o no a un modelo de la base de datos, se evalúa la magnitud del parecido entre dicha información y el modelo que da mejor resultado en la comparación. Si esta semejanza supera un umbral determinado, se considerará que la información corresponde al modelo. Si por el contrario esta semejanza no supera el umbral establecido, se considerará que la información adquirida no corresponde a ningún patrón almacenado en la base de datos.

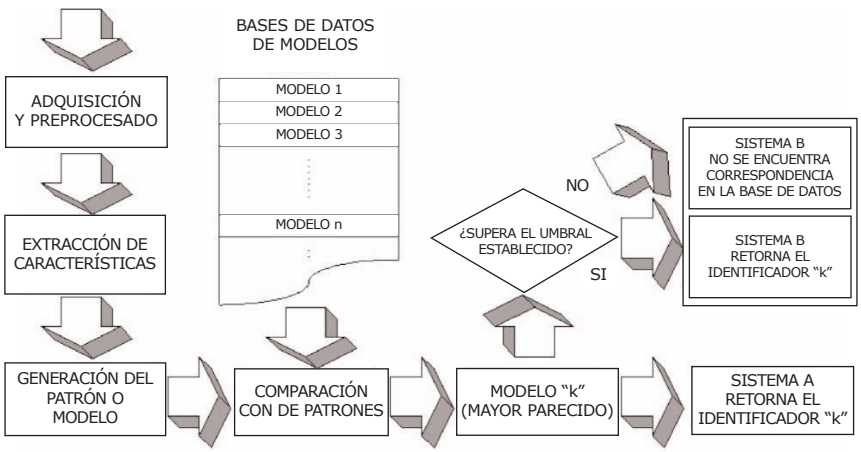


Figura 4. Operación en Modo Identificación.

El funcionamiento en modo identificación se utiliza para el "reconocimiento negativo", donde el sistema ha de establecer si una persona es quien (implícita o explícitamente) niega ser. El propósito del reconocimiento negativo es evitar que un único individuo utilice varias identidades. El modo identificación también puede utilizarse en reconocimiento positivo para comodidad del usuario (no se le pide al usuario que solicite ninguna identidad pretendida). Ejemplos de aplicaciones que funcionan en modo identificación son el control de fronteras, la investigación criminal sobre grandes bases de datos, identificación de personas perdidas, etc. Mientras que el reconocimiento positivo puede realizarse también con los métodos tradicionales (llaves, números PIN, etc.), el reconocimiento negativo solamente puede llevarse a cabo mediante el reconocimiento biométrico.

Modo vigilancia, screening o black-listing (¿es esta una persona buscada?): las aplicaciones de vigilancia determinan si un individuo se encuentra dentro de una lista de personas buscadas, por ejemplo en control de seguridad en aeropuertos, seguridad en eventos públicos, etc. Se trata de un caso particular del modo identificación en conjunto abierto donde la lista de personas suele tener un tamaño moderado (por ejemplo cientos de identidades) y no puede esperarse tener control sobre la calidad de los datos contenidos en la lista (típicamente obtenidos en escenas de crimen, en material incautado mediante detenciones, etc.)

2.3. Rendimiento de un sistema biométrico

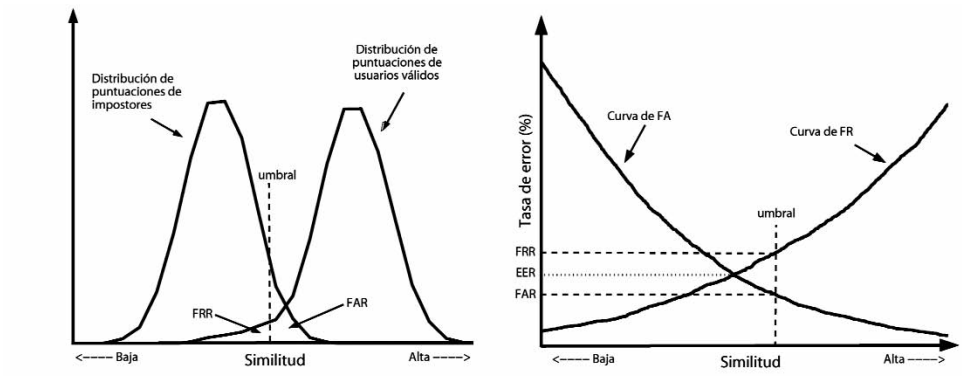
Dos muestras o patrones de un mismo rasgo biométrico nunca son exactamente iguales debido a imperfecciones en las condiciones en las que se captura la imagen, a cambios en los rasgos fisiológicos o de comportamiento del usuario, a factores ambientales, a la interacción del usuario con el sensor, etc. Por tanto, la respuesta del comparador de un sistema biométrico consiste en una puntuación o "score" que cuantifica la similitud entre ambas muestras o patrones. Cuanto mayor sea el parecido, mayor será la puntuación devuelta por el comparador y más seguro estará el sistema de que las dos medidas biométricas pertenecen a la misma persona. La decisión del sistema está regulada por un umbral: las muestras o patrones cuya comparación genere puntuaciones mayores o iguales que el umbral se supondrán correspondientes a la misma persona, mientras que si la puntuación es menor que el umbral, se considerarán de personas diferentes.

Cuando se diseña un sistema de reconocimiento automático es muy importante saber cómo medir de una forma fiable y precisa su rendimiento.

Esto es fundamental para determinar si el sistema diseñado cumple unos requisitos mínimos especificados o para compararlo con otros sistemas con el fin de encontrar el más adecuado para una aplicación específica. Para llevar a cabo una evaluación objetiva de un sistema es necesario realizar unas pruebas sobre el mismo, simulando unas condiciones lo más parecidas a las estándar y empleando unos datos de entrada controlados para los cuales se conoce a priori la salida correcta. Como resultado de la evaluación, se mide la eficiencia del sistema mediante unas tasas estadísticas de error. A continuación, describiremos los mecanismos de evaluación de un sistema biométrico, así como la terminología utilizada para notificar las tasas de error del mismo [45].

Rendimiento en modo verificación

Ya hemos dicho que la respuesta del comparador de un sistema biométrico es una puntuación, tanto más alta cuanto más parecido haya entre las muestras o patrones biométricos bajo comparación. La distribución de puntuaciones generadas por comparaciones entre muestras o patrones de la misma persona se llama **distribución de usuarios válidos** y la distribución de puntuaciones generadas por muestras o patrones de diferentes personas se llama **distribución de impostores**, tal como se muestra en la Figura 5a. En un sistema ideal, los rangos de variación de las puntuaciones obtenidas para usuarios válidos e impostores están separados, de manera que no hay solapamiento entre sus distribuciones, pudiéndose establecer un umbral de decisión que discrimine perfectamente entre ambas clases. Sin embargo, en un sistema real siempre existe una región en la que se solapan ambas distribuciones.



(a) (b)

Figura 5. (a) Distribuciones de puntuaciones de usuarios válidos e impostores. (b) Errores FA y FR en función del umbral de similitud.

Si se fija un umbral (ver Figura 5a), todas las puntuaciones, tanto de usuarios como de impostores, cuyo valor sea superior a ese umbral serán interpretadas por el sistema como usuarios registrados. Como consecuencia, el área bajo la curva de impostores que queda por encima del umbral es la probabilidad de que un impostor sea aceptado y se conoce como la **Tasa de Falsa Aceptación** (en inglés, False Acceptance Rate o **FAR**). Este error se produce cuando el sistema indica que las dos muestras comparadas se corresponden con la misma identidad, cuando realmente no se corresponden. Complementariamente, el área bajo la curva de usuarios validos que queda por debajo del umbral es la probabilidad de que un usuario registrado no sea aceptado por el sistema y se denomina **Tasa de Falso Rechazo** (en inglés, False Rejection Rate o **FRR**). Este error se produce cuando el sistema indica que las dos muestras comparadas no se corresponden con la misma identidad, cuando realmente sí se corresponden. Así, para cada valor que se fije del umbral, se obtiene simultáneamente un valor de FAR y otro de FRR, lo cual se muestra en la Figura 5b. Como medida conjunta de ambos tipos de error, los sistemas se suelen caracterizar mediante la **Tasa de Igual Error** (en inglés, Equal Error Rate o **EER**), que es el punto en el que la FAR y la FRR son iguales. Cuanto menos solapadas estén las distribuciones de usuarios válidos y de impostores, menor será el EER. Por tanto, como medida comparativa entre varios sistemas, cuanto menor sea el valor de EER, mejor es el sistema.

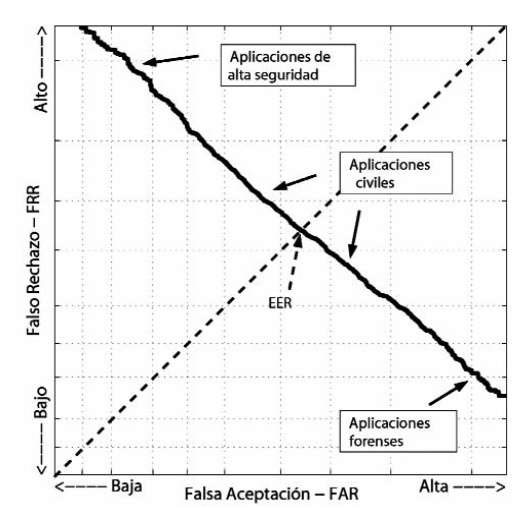


Figura 6. Curva DET.

Otra forma de representar el rendimiento de un sistema es la **curva DET** (en inglés, *Detection Error Tradeoff*). Dicha curva consiste en representar la FAR y la FRR conjuntamente para todos los posibles valores del umbral, como se ve en la Figura 6. La ventaja es que tenemos ambos tipos de error en una única curva, aunque como contrapartida se pierde la información acerca del valor del umbral. El valor del EER se extrae a partir de la curva DET como el punto en el que ésta corta a la bisectriz de la gráfica, tal como se indica en la Figura 6.

Hay que hacer especial hincapié en el compromiso que existe entre la FAR y la FRR, ya que según se sitúe el umbral, ambas varían de manera totalmente opuesta. Si se fija un valor del umbral alto para que el sistema sea seguro y no se "cuelen" impostores (falsa aceptación baja), se reduce la permisividad con los usuarios válidos (el falso rechazo será alto). Esta es la situación típica en entornos de alta seguridad, como indica en la Figura 6 (por ejemplo, control de acceso a instalaciones sensibles). El objetivo en este tipo de entornos es evitar que accedan personas no autorizadas, aun a costa de que haya menos permisividad con los usuarios auténticos (Ej.: "ponga su huella otra vez" o "vuelva a decir su clave" o "espere a que acuda un operador manual"). Por el contrario, si se fija un valor del umbral bajo, el sistema será tolerante con los usuarios válidos (el falso rechazo será bajo) pero a su vez, permitirá que se "cuelen" más impostores (la falsa aceptación será alta). Esta es la situación típica en aplicaciones forenses o policiales (ver Figura 6), por ejemplo a la hora de buscar si un individuo se encuentra dentro de una lista de criminales buscados. El objetivo en estas aplicaciones es que si el individuo está en la lista, el sistema sea capaz de averiguarlo (falso rechazo bajo), aun a costa de que obtenga *falsas aceptaciones* con personas que realmente no están en la lista. En este tipo de situaciones, siempre hay un operario (un agente o un perito) que se encarga de resolver manualmente la *alarma*, entendiendo que una alarma dada por el sistema no significa directamente que estemos ante un criminal. Por último, la mayoría de aplicaciones civiles tienen su punto de trabajo en una situación intermedia (ver Figura 6), donde la FAR y la FRR no toman valores dispares una de la otra.

Rendimiento en modo identificación

En modo identificación, el sistema tiene que comparar los datos de entrada con los N modelos de identidad almacenados en la base de datos, devolviendo el modelo con mayor parecido. En este caso, el rendimiento se indica en términos de tasa de acierto, medida como el porcentaje de veces que el modelo devuelto por el sistema es el correcto. Hay que tener en cuenta que solamente hay un modelo de identidad en la base de datos que se corresponde con los datos de entrada, mientras que hay N - 1

modelos que corresponden a otras identidades. De esto se deduce que si el tamaño de la base de datos es muy grande, la tasa de acierto del sistema puede decrecer considerablemente, ya que hay más modelos de otras identidades con los que comparar y por tanto, mayor probabilidad de cometer un error. Esto puede suponer un problema por ejemplo en reconocimiento negativo, donde sólo es posible trabajar en modo identificación. Una posible opción es que el sistema no devuelva una sola identidad como resultado, sino una lista de varias, por ejemplo de 10 ó 20 identidades, aumentando así las posibilidades de que la identidad buscada se encuentre dentro de esta lista. A continuación un operador manual efectuará la decisión final a partir de dicha lista. En este caso, a pesar de que tenga que haber intervención humana en la decisión, el sistema nos evita tener que buscar manualmente en un conjunto de N identidades (que pueden ser millones), reduciendo la búsqueda a solamente 10 ó 20.

Otros errores

Aparte de los errores básicos de Falsa Aceptación y Falso Rechazo, hay otro tipo de errores asociados con situaciones de funcionamiento específicas de los sistemas biométricos, tanto en verificación como en identificación [14]:

- **Error de Fallo en Adquisición** (en inglés, *Failure to Acquire* o **FTA**): Es el porcentaje de población que no posee un rasgo biométrico particular (Ej. a un usuario le falta el dedo) o que no es capaz de proporcionar un rasgo utilizable (Ej. tiene el dedo dañado). En el primer caso, no hay solución posible, mientras que en el segundo caso pudiera ser que la tecnología avanzara lo suficiente como para poder capturar a ese usuario. También sucede cuando, por alguna razón, el sistema no es capaz de capturar adecuadamente el rasgo biométrico cuando se le presenta (Ej. si el usuario no pone correctamente el dedo en el sensor).

- **Error de Fallo en Registro** (en inglés, *Failure to Enroll* o **FTE**): Es el porcentaje de población de la cual no es posible generar un modelo de identidad fiable. Sucede típicamente cuando el sistema rechaza muestras de baja calidad para el registro. La consecuencia de aplicar este mecanismo es que la base de datos contiene solamente modelos de buena calidad, lo cual artificialmente mejora el rendimiento del sistema a costa de aumentar la inconveniencia para el usuario y el coste de tener que aplicar otro mecanismo de autenticación.

Hay que notar que ambos errores, FTA y FTE, tienen que ver en parte con limitaciones intrínsecas de los sistemas biométricos y con el estado de la tecnología. Igualmente, tienen fuerte relación con los errores básicos de Falsa Aceptación y Falso Rechazo y los cuatro errores -FAR, FRR, FTA y FTE- constituyen importantes especificaciones de un sistema biométrico que no deben dejar de proporcionarse a la hora de medir su rendimiento. Por ejemplo, si tengo dos sistemas biométricos con idénticas tasas de FAR y FRR pero distinta tasa de FTE, quiere decirse que uno de ellos es capaz de procesar mejor las muestras de baja calidad.

Compromisos de diseño

Los dos tipos de error básicos de un sistema (Falsa Aceptación y Falso Rechazo) afectan a diferente tipo de gente. Una falsa aceptación significa que una persona no autorizada ha conseguido acceder al sistema (una brecha de seguridad). Por contra, un falso rechazo significa que se le ha negado el acceso a un usuario autorizado, lo cual no afecta a la seguridad pero supone una molestia para el usuario implicado y un inconveniente al normal desarrollo de su actividad (como ya dijimos antes, por ejemplo, "ponga su huella otra vez" o "vuelva a decir su clave" o "espere a que acuda un operador manual"). Por tanto, el compromiso entre FAR y FRR se refleja a su vez en otro compromiso entre seguridad y conveniencia (en el sentido de comodidad de uso) [14].

- **Conveniencia vs. Seguridad**: Por conveniencia entendemos la comodidad que le supone a un usuario autorizado el uso del sistema. Según esto, podemos definir la siguiente medida de conveniencia:

  $$Conveniencia = 1 - FRR$$

  Cuanto mayor sea la FRR, menos conveniente será un sistema puesto que un mayor número de individuos autorizados son incorrectamente rechazados. Igualmente, la FAR está relacionada con la seguridad del sistema:

  $$Seguridad = 1 - FAR$$

  Por tanto, como ya hemos dicho, hay un compromiso entre seguridad y conveniencia a la hora de diseñar un sistema biométrico.

- **Coste vs. Seguridad**: Igualmente importante es el compromiso entre coste y seguridad de un sistema biométrico. Si elegimos un punto de trabajo extremo donde FRR=0 % y FAR=100 %, tenemos un sistema muy barato pero totalmente inseguro. Por contra, si elegimos FAR=0%

y FRR=100%, el sistema no acepta a nadie y es necesario que todos los accesos sean comprobados por operarios manuales. Por tanto, la FRR puede usarse como definición del coste de un sistema:

$$Coste = FRR$$

Cuanto mayor sea la FRR, mayor es el coste de un sistema, puesto que más usuarios autorizados son incorrectamente rechazados, teniendo que invocar algún mecanismo de excepción, como que acuda un operario manual.

2.4. Evaluaciones competitivas

Si bien los sistemas biométricos automáticos se llevan desarrollando décadas, hasta hace pocos años las únicas medidas de rendimiento de los mismos eran las proporcionadas por sus propios creadores. Como cada desarrollador realizaba sus propias pruebas, usualmente no accesibles a terceros, no era posible establecer un marco comparativo fiable entre distintos sistemas biométricos.

Afortunadamente, en los últimos años han ido surgiendo una serie de evaluaciones competitivas, realizadas por instituciones independientes, que han proporcionado marcos objetivos para la comparación de sistemas biométricos. También han ido surgiendo una serie de propuestas sobre prácticas y criterios comunes de evaluación [51, 78]. Aun no tratándose de estándares estrictos, muchas de las bases de datos y protocolos usados en este tipo de evaluaciones se convierten en estándares *de facto*, de tal manera que los desarrollos posteriores a la evaluación suelen usarlos para sus pruebas, ayudando así a una comparación y valoración más objetiva. A su vez, la existencia de estas evaluaciones competitivas suele servir de acicate a los grupos de investigación, de tal manera que el desarrollo tecnológico suele ser mayor ante la presencia de este tipo de evaluaciones.

En cuanto a especialización del estudio, distinguimos tres tipos de evaluación [14]:

- **Evaluación tecnológica**: Es la más general y se realiza sobre unos datos cerrados previamente capturados. Su objetivo es medir el estado de la tecnología, determinar su progreso e identificar los enfoques más prometedores. La ventaja es que, al usarse un conjunto de datos cerrado, la evaluación puede repetirse tantas veces como sea necesario. Las bases de datos que se utilicen no deben ser conocidas de antemano por los participantes, aunque se suele proporcionar un subconjunto de datos de características similares

a los que luego se usarán en la evaluación, con el fin de que los participantes puedan ajustar sus sistemas. Las bases de datos deben crearse con unas características tales que la evaluación no sea ni muy fácil ni muy difícil de acuerdo con el estado tecnológico en ese momento. Ejemplo de evaluaciones estándar de este tipo son:

- *Fingerprint Verification Competition - FVC*, de huella, realizada con carácter bianual los años 2000, 2002, 2004 y 2006 [34].

- *Signature Verification Competition - SVC*, de firma, en el año 2004 [74].

- *Face Recognition Vendor Test - FRVT*, de cara, realizada en los años 2000, 2002 y 2006 [32].

- *NIST Speaker Recognition Evaluation - SRE*, de voz, es la competición más veterana, con ediciones anuales desde 1996 [56].

- *Iris Challenge Evaluation - ICE*, de iris, en 2005 y 2006 [37].

- *Biosecure Multimodal Evaluation Campaign*, recientemente celebrada en 2007 [13].

- **Evaluación de escenario**: Se mide el rendimiento del sistema para un escenario prototipo que simula una determinada aplicación, con el objetivo de determinar si la tecnología está lo bastante madura para cumplir los requisitos de funcionamiento de dicha aplicación. A diferencia de la evaluación anterior, no se incluyen solamente los algoritmos de reconocimiento, sino que se extiende a todo el sistema incluyendo la etapa de captura (sensores, control de calidad de la muestra, etc.). Cada sistema incluye sus propios sensores, de manera que serán probados sobre muestras de datos ligeramente distintas. Esto y el hecho de que la evaluación se haga bajo condiciones reales, hacen que no sea completamente repetible. Hay que prestar atención para que todos los sistemas sean probados por la misma población y en el mismo entorno, de manera que los resultados sean más objetivos. Un ejemplo de evaluación de este tipo en la que se evalúan 7 sistemas biométricos distintos es [52].

- **Evaluación operacional**: Es similar a la de escenario pero para un sistema concreto, en un entorno totalmente real y para una población determinada. Su objetivo es determinar si el sistema biométrico evaluado cumple con los requisitos de una determinada aplicación.

Para que una evaluación sea realmente objetiva, debe ser realizada por instituciones independientes. Lo ideal sería que las pruebas se realizaran sobre todo posible usuario del sistema, ya que sólo así se tendría una medida real de su rendimiento. Esto, no obstante, es imposible en la práctica, por lo que las pruebas se realizan sobre un subconjunto de individuos. La composición de este subconjunto condiciona enormemente el alcance de la evaluación así como la representatividad de sus resultados, razón por la que es importante fijar con cuidado este subconjunto y conocer su composición a la hora de valorar los resultados. Con carácter general, acerca de los datos usados para la evaluación podemos decir que:

- No es aconsejable el uso de muestras artificiales, ya que los resultados no serán extrapolables a la realidad (Ej. voces sintetizadas, caras creadas digitalmente, etc.)

- Un buen mecanismo es minimizar la intervención humana en su captura, pues puede añadir subjetividad (Ej. decidir sobre la calidad de una muestra). Cuanto más se automatice el proceso, más cerca de la situación real de uso estarán los datos. En caso de que haya algún tipo de intervención humana, ésta debe estar claramente definida bajo criterios concretos.

- Hay que definir y conocer el entorno en el que se han adquirido los datos (condiciones de iluminación, condiciones ambientales, ruido presente, posibles perturbaciones, etc.) así como la población que compone los datos. Ambos aspectos deben ser los suficientemente representativos y genéricos como para poder evaluar objetivamente y de un modo real los diferentes sistemas. Por otro lado, hay que tener en cuenta el estado de la tecnología en ese momento para que los datos no sean ni muy fáciles ni muy difíciles. Hay que prestar también atención para que los casos especiales estén correctamente representados (por ejemplo, huellas de trabajadores manuales), de modo que no aparezcan sesgos en los resultados.

Capítulo 3

Modalidades biométricas

3. Modalidades biométricas

En este capítulo haremos una descripción de los diferentes rasgos biométricos [44, 45], sin entrar en un nivel de detalle profundo, pero a la vez destacando sus características más relevantes, así como sus ventajas e inconvenientes [53]. En primer lugar, hablaremos de los rasgos más utilizados [14]: huella, cara, voz, geometría de la mano, iris y firma. Posteriormente, hablaremos de otros rasgos biométricos adicionales como la forma de andar, la forma de teclear o la geometría de la oreja.

3.1. Rasgos más utilizados

Huella dactilar

La huella dactilar se ha usado durante décadas para identificación personal, alcanzando en la actualidad una precisión muy alta en el reconocimiento [50]. De hecho, la mitad de las inversiones en el mercado del reconocimiento biométrico corresponden a la huella dactilar [36], puesto que la mayoría de las fuerzas de seguridad de todo el mundo mantienen y utilizan bases de datos de huellas dactilares. La huella dactilar se compone de un patrón de crestas y valles situadas en la superficie del dedo (ver Figura 7(a)) el cual se forma durante los primeros meses de desarrollo fetal y permanece hasta la descomposición tras la muerte. Asimismo, la sudoración, la secreción sebácea y la suciedad de la piel hacen que el contacto del dedo con casi cualquier superficie (metal, cristal, plástico, madera, etc.) produzca en la misma una huella latente que puede ser posteriormente capturada.

(a) (b)

Figura 7. (a) ejemplo de huella, (b) ejemplo de huella de baja calidad.

La mayoría de los sistemas automáticos de huella hacen uso de dos características particulares del patrón de crestas y valles: el fin de cresta (Figura 8(a)) y la bifurcación de crestas (Figura 8(b)). Estas dos características son conocidas como puntos característicos o minucias (en inglés, *minutiae*) y su uso en sistemas automáticos se debe a que es el mecanismo utilizado desde hace siglos en entornos policiales y forenses.

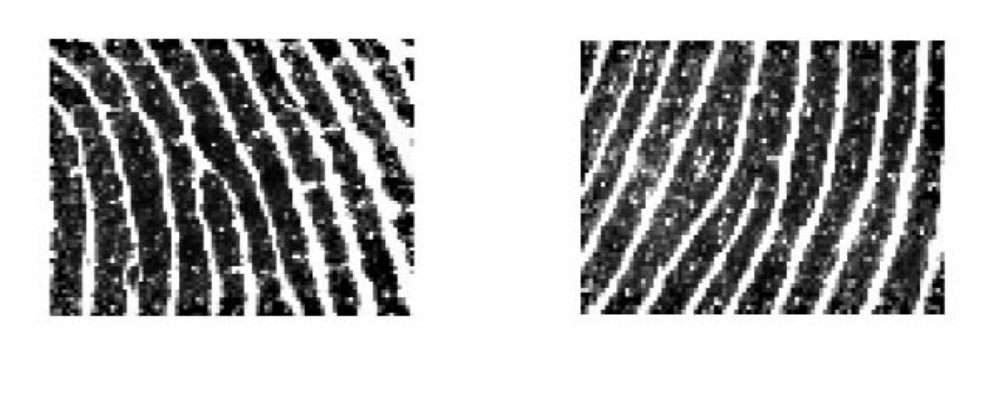


Figura 8. (a) fin de cresta, (b) bifurcación de cresta.

Tradicionalmente la huella se ha capturado impregnando el dedo en tinta y haciéndolo rodar en un papel, por lo que para su uso en sistemas automáticos es preciso primero digitalizar las huellas con un escáner de documentos. En las últimas décadas se han desarrollado sensores electrónicos que capturan la huella sin utilizar tinta y directamente producen una imagen digital. Actualmente hay sensores de bajo coste y pequeños, habiendo incluso dispositivos portátiles que ya integran uno (por ejemplo, ordenadores portátiles, teléfonos móviles, etc.). A pesar de sus ventajas, la huella puede presentar baja aceptación en algún caso por su potencial asociación con la investigación criminal. Existe asimismo una fracción de población cuyas huellas puede que no sean adecuadas para el reconocimiento, como los trabajadores manuales, o incluso personas que no tengan huellas (quemaduras o dedos amputados). Bajo ciertas condiciones, también puede suceder que no obtengamos huellas de buena calidad, como en la Figura 7(b), debido a que el dedo puede estar húmedo o seco, o bien a que puede haber suciedad en el sensor o en el propio dedo.

Igualmente, el hecho de tener que apoyar el dedo contra un sensor puede provocar rechazo debido a problemas de higiene o contacto con una superficie utilizada por otras personas.

Reconocimiento de cara

La cara es un mecanismo no intrusivo de reconocimiento que no exige contacto con el sensor y quizá es, junto con la voz, el método más natural utilizado por las personas para el reconocimiento. Es un mecanismo ampliamente aceptado dado su uso en pasaportes, DNI, permisos de conducir, etc. Los algoritmos de reconocimiento de cara más habituales [49] están basados en la localización y forma de los atributos faciales (ojos, nariz, labios, barbilla, etc.) así como sus relaciones espaciales, o bien en un análisis global de la misma, representándola como combinación de un conjunto de caras de referencia llamadas canónicas (*eigenfaces*).

Los sistemas de reconocimiento de cara han alcanzado un rendimiento aceptable para su uso comercial, pero presentan una serie de restricciones de funcionamiento. Cuando la iluminación, la pose de la cara o el fondo de la imagen no se controlan, el rendimiento se degrada considerablemente. El reconocimiento de cara puede incluso utilizarse sin que el usuario se entere, en cuyo caso podrían plantearse problemas de privacidad o de aceptación. Para la captura de la imagen de cara puede utilizarse una cámara fotográfica o una cámara de video capaz de capturar fotos. En la actualidad existen sistemas capaces de producir imágenes de la cara en tres dimensiones mediante la combinación imágenes procedentes de varias cámaras e igualmente, para contrarrestar la influencia de la iluminación, hay cámaras que capturan imágenes infrarrojas de la cara. No obstante, junto al mejor rendimiento que ello produce, tenemos un incremento en el coste del dispositivo de captura.

Reconocimiento de voz

La voz es una combinación de características fisiológicas y de comportamiento. Las características fisiológicas vienen dadas por la forma y tamaño de las cavidades del tracto vocal (boca, fosas nasales, laringe, etc.) y son estables para cada individuo. Las características de comportamiento sin embargo pueden ser muy variables con el tiempo y dependen de factores tales como el estado de ánimo, la edad, el contexto social o posibles enfermedades que afecten a la voz (un resfriado). Esto hace que la voz no sea un rasgo con una capacidad discriminativa comparable, p.e., a la huella

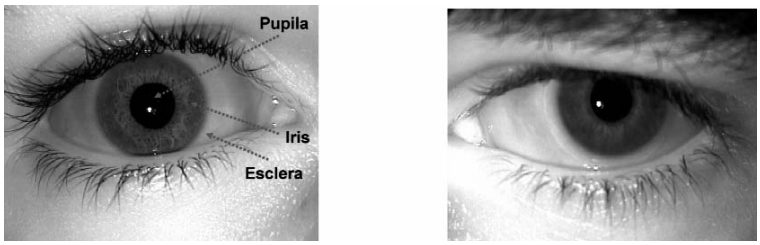
dactilar, pero a cambio es muy sencilla de obtener con un micrófono o a través del canal telefónico (fijo o móvil). En este sentido, resulta ideal para aplicaciones como la gestión automática de servicios (telecompra, reserva de billetes, información telefónica) o la interacción remota con dispositivos. Al igual que la cara, la voz se obtiene de manera no intrusiva e incluso puede suceder que el usuario no se entere de que está siendo capturado. Por contra, es sensible a factores como el ruido ambiente o la calidad e interferencias del micrófono o del canal telefónico. También existe la posibilidad de que un individuo no pueda hablar debido a diversas enfermedades.

En función de la complejidad del sistema, podemos distinguir entre sistemas de voz *dependientes de texto*, en los cuales el usuario debe decir una determinada palabra o frase (ejemplo: un número secreto o PIN), y sistemas de voz *independientes de texto*, donde se permite al usuario decir lo que quiera. El segundo tipo de sistemas es más complejo de diseñar, dado que no hay restricciones a lo que el usuario debe decir.

En teoría, se podría pensar en una posible vulnerabilidad de este tipo de sistemas mediante la imitación de la voz de un individuo, o incluso mediante la grabación y posterior reproducción de un determinado mensaje hablado. Para combatirlo, los sistemas modernos son capaces de analizar la entonación, el ritmo del habla e incluso el léxico, la jerga o la repetición de expresiones típicas de cada individuo; asimismo, son capaces de proponer de forma dinámica una determinada locución, evitando así el uso de posibles grabaciones previas. En este sentido, los sistemas independientes de texto proporcionan mayor robustez, puesto que al poder decir el usuario lo que quiera, se obtiene un habla más natural y característico de la persona.

Reconocimiento de iris

El iris es la región anular del ojo que se encuentra entre la pupila (el círculo negro central) y la esclera (la parte blanca externa), (ver Figura 9(a)). La textura que posee el iris se forma durante el desarrollo fetal y se estabiliza durante los dos primeros años de vida. La complejidad y riqueza de información que posee dicha textura hace que sea un rasgo muy distintivo, obteniendo un rendimiento muy elevado. El iris se presenta ante la comunidad científica como el rasgo biométrico más identificativo (a excepción del ADN, si bien éste no suele considerarse un rasgo biométrico en aplicaciones civiles, al no permitir el reconocimiento en tiempo real), si bien recientes evaluaciones competitivas han puesto en entredicho este presupuesto. Otra ventaja del iris es que su captura no precisa contacto físico con el sensor.



(a) (b)

Figura 9. (a) ejemplo de iris (b) ejemplo de iris ocluido.

Como contrapartida, el iris tiene un tamaño muy pequeño, por lo que el usuario debe cooperar situándose cerca del dispositivo de captura (menos de medio metro) y los sensores de adquisición suelen ser caros. Asimismo, las gafas y las lentes de contacto afectan al rendimiento del sistema, siendo necesario que el usuario se las quite. Otro problema aparece cuando las pestañas o los párpados tapan parte del iris, como se ve en la Figura 9(b), algo que es muy característico en individuos orientales.

Geometría de la mano

El reconocimiento mediante geometría de la mano se basa en una serie de medidas tales como la forma de la mano, el tamaño de la palma y la longitud y anchura de los dedos, tal como puede observarse en la Figura 10. El coste del sistema de captura es muy bajo, ya que solo hay que fotografiar la mano, y a diferencia de la huella, el impacto de factores como la humedad o la suciedad es mínimo.

La geometría de la mano es un rasgo que no proporciona una altísima capacidad de discriminación y es variable durante la etapa de crecimiento. Igualmente, existe el impacto de elementos como joyas, anillos, limitaciones de movilidad en caso de artritis e incluso posible falta de algún dedo o de la mano entera. El sensor es bastante grande, puesto que debe ponerse toda la mano, y su uso puede plantear aún más rechazo que la huella por cuestiones de higiene. Por el contrario, hay factores que juegan a favor de la aceptación de la mano como rasgo de identificación. Uno de ellos es la operación en modo "hágalo usted mismo", donde el usuario pone la mano extendida sin que sea necesaria supervisión. Otro factor es el hecho de que la mano no tenga connotaciones criminales, policiales o de invasión de intimidad que sí tienen otros rasgos más distintivos como la huella o el iris.

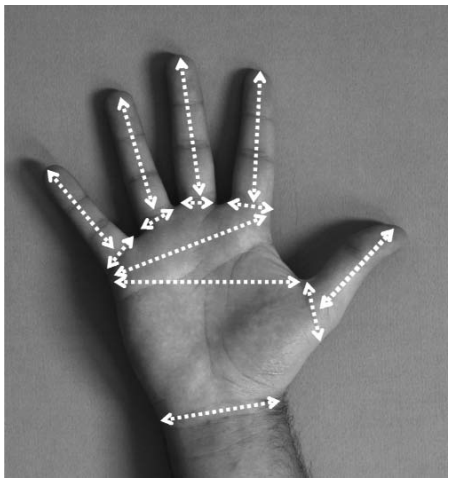
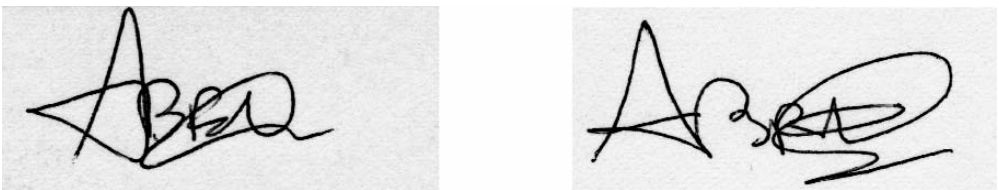


Figura 10. Geometría de la mano.

Firma manuscrita

La firma de una persona, así como la manera en que realiza dicha firma, es una propiedad característica de cada individuo. La firma es un mecanismo de validación de identidad usado desde hace siglos en entornos legales, gubernamentales y en transacciones comerciales. Es por ello que su aceptación como mecanismo de reconocimiento es muy alta. Por el contrario, la firma es un rasgo de comportamiento que va cambiando con el tiempo, que depende del estado físico y emocional, y que precisa que el individuo coopere y realice el acto de firmar. Incluso varias firmas hechas en un corto espacio de tiempo pueden diferir sustancialmente. Asimismo, la firma es susceptible de ser imitada (ver Figura 11).



(a) (b)

Figura 11. (a) ejemplo de firma, (b) ejemplo de imitación.

En términos del mecanismo de captura, se distinguen los siguientes sistemas de reconocimiento basados en firma:

1. Sistemas *off-line* o estáticos, donde las firmas se hacen en papel y posteriormente son escaneadas para su tratamiento automático.

2. Sistemas *on-line* o dinámicos, donde la firma se realiza sobre una superficie capaz de capturar el desplazamiento del bolígrafo y la presión que se ejerce, incluso si el bolígrafo no está en contacto con la superficie.

Los sistemas *off-line* solamente disponen de la imagen final de la firma. Al no haber información acerca del proceso de realización de la firma, son más vulnerables a imitaciones. Por el contrario, los sistemas on-line [31] son menos vulnerables, al tener tanto la imagen final de la firma como el proceso de realización de la misma. Este tipo de sistemas hacen uso de tabletas digitalizadoras que se conectan a un terminal PC, o incluso de los modernos dispositivos portátiles que incorporan pantallas con posibilidad de captura mediante un lápiz (teléfonos móviles, PDA, etc.).

3.2. Otros rasgos biométricos

El avance de la tecnología y la creciente demanda de aplicaciones de reconocimiento de personas han dado lugar a un gran número de modalidades biométricas. En la sección anterior hemos descrito los rasgos principales, considerando como tal los más utilizados y/o los que mayor precisión de reconocimiento proporcionan. En esta sección presentaremos una lista de otros rasgos biométricos que han ido recibiendo creciente atención en los últimos años.

ADN

El ADN es un rasgo ampliamente utilizado en entornos forenses y policiales. No obstante, presenta una serie de inconvenientes que limitan su uso en otras aplicaciones. Incluso hay autores que por esa razón no lo consideran un rasgo biométrico propiamente dicho. En primer lugar, presenta problemas de privacidad importantes, ya que a partir del ADN puede extraerse información sobre ciertas enfermedades. Por otro lado, el reconocimiento ha de realizarlo un experto en un laboratorio químico, proceso que puede llevar al menos varias horas. Es por ello que en este momento no hay posibilidad de tener un sistema totalmente automático, barato y que permita operar en tiempo real.

Escáner de retina

La retina se encuentra en la parte posterior del globo ocular. El patrón de capilares existente en la retina se considera propio e individual de cada persona. Para su captura es necesario enfocar con haces de luz infrarroja a través del cristalino, requiriendo fuerte cooperación por parte del usuario, el cual tiene que situar el ojo a pocos centímetros del sensor. Otro factor en contra es que el patrón vascular de la retina puede revelar algunas enfermedades como hipertensión. No obstante, este rasgo biométrico se considera como de alta seguridad, puesto que no es fácil de alterar o de replicar.

Modo de andar

El modo de andar es una característica peculiar de cada persona. A pesar de que no es muy distintivo, es muy fácil de capturar (basta una cámara de vídeo) y no es necesaria la cooperación del usuario. Pensemos que en sistemas de control de acceso en los que existan cámaras ya instaladas, será un rasgo adicional fácilmente obtenible. No obstante, al ser una característica de comportamiento, está sujeta a variaciones con el tiempo debido a cambios en el peso, vestimenta, lesiones, enfermedades, estados de embriaguez, etc.

Dinámica de tecleo

Es posible pensar que cada persona escribe con un teclado de manera diferente, mostrando diferencias en el tiempo transcurrido entre cada pulsación o el tiempo que se tiene pulsada cada tecla. No es un rasgo de muy alta capacidad discriminativa y puede ser variable al tratarse de una característica de comportamiento. Por el contrario, puede obtenerse de un modo no intrusivo (simplemente monitorizando al usuario) y al poder observarse durante un periodo de tiempo más o menos largo, permite verificar la identidad del usuario a lo largo de todo ese tiempo. Por ejemplo, si en un momento dado se observan cambios importantes en la dinámica de tecleo, puede considerarse que el usuario no es el mismo y a continuación, bloquear el sistema.

Forma de la oreja

Se ha sugerido que la forma de la oreja así como su estructura de cartílagos es un rasgo que permite distinguir entre personas. No es un rasgo muy distintivo, pero su captura es bastante sencilla y no sufre los problemas de iluminación o del fondo que tiene el reconocimiento de cara, puesto que la propia cabeza alrededor de la oreja actúa como fondo, permitiendo detectarla de un modo fiable.

Movimiento de los labios

El movimiento de los labios es una característica de comportamiento que analiza los movimientos a medida que el individuo va hablando. Puede combinarse muy fácilmente con la voz y/o con una secuencia de imágenes (vídeo) de la cara. Esta triple combinación da lugar a un sistema muy difícil de vulnerar y que solamente necesita una cámara de vídeo con micrófono que capture al usuario hablando. Al igual que los sistemas de voz, puede trabajar en modo dependiente de texto o en modo independiente de texto. Asimismo, para la captura de los labios, como para la cara, pueden usarse cámaras con luz visible o con luz infrarroja.

Olor

El olor del individuo es una característica de reconocimiento que se ha usado desde hace mucho tiempo con perros adiestrados. Actualmente existen "narices electrónicas" que permiten identificar la existencia en el aire de diferentes elementos químicos que puedan componer el olor de un individuo. No obstante, aún no proporcionan la precisión de la nariz humana y también se sabe que el olor de una persona puede verse influenciado por estados de salud, higiene, uso de diferentes perfumes, jabones, etc.

3.3. Elección del rasgo biométrico adecuado

La elección de un rasgo biométrico para una aplicación no ha de basarse solamente en su posible capacidad discriminativa. A la hora de elegir, concurren muchos factores adicionales como el coste, el nivel de seguridad requerido, el tiempo de respuesta necesario, la aplicación, etc. (ver Figura 12). Aun cuando la tasa de error dada por un rasgo biométrico es importante, en modo alguno tiene porque ser el factor único o decisivo a la hora de optar por una u otra modalidad biométrica [14].

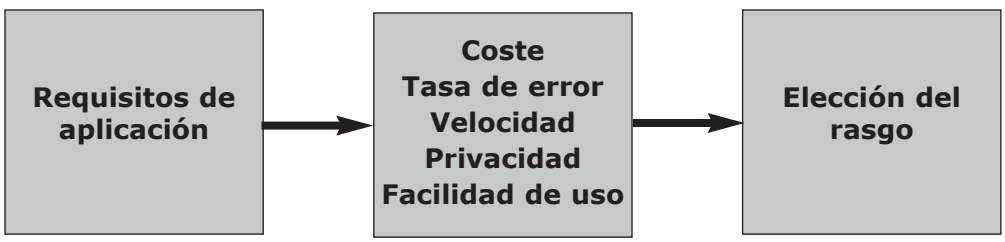


Figura 12. Elegir el rasgo biométrico adecuado es una decisión que implica múltiples factores.

Factores que afectan al rasgo biométrico

Hay una serie de atributos de los rasgos biométricos que afectan a la hora de elegir uno u otro rasgo. Uno de los más importantes, que también resulta complicado de medir, se refiere a la **madurez** de la tecnología implicada. Aquí confluyen elementos tales como:

- que la tecnología permita capturar el rasgo y llevar a cabo el reconocimiento con calidad y precisión suficientes.

- el conocimiento de los factores que pueden afectar a la variabilidad o a la degradación de un rasgo, así como la existencia de soluciones que puedan hacerles frente (por ejemplo, el ruido de fondo en voz o la captura de imágenes de cara donde no se controla la iluminación).

- en general, que se tenga un profundo conocimiento del rasgo biométrico, de todos los factores que puedan aparecer a la hora de ser usado y de la manera de darles respuesta; en este sentido, rasgos tales como la huella o la voz tienen una larga tradición de estudio y utilización, a diferencia de otros rasgos más recientes como el modo de andar o de teclear.

En definitiva, la madurez de un rasgo biométrico tendría impacto en la disponibilidad de distintas soluciones y productos, lo cual a su vez redunda en la elección de ese rasgo frente a otro. Otro atributo importante de un rasgo que puede condicionar su elección se refiere a las **propiedades del sensor**:

- Si requiere contacto o no. En caso de requerir contacto, es necesaria la cooperación del sujeto, mientras que si no requiere contacto podría usarse incluso sin que el usuario lo perciba. Si necesita contacto, puede plantear problemas de rechazo por motivos de higiene.

- Tamaño del sensor. Algunos rasgos biométricos pueden utilizar sensores bastante pequeños y baratos (huella, cara, voz), por lo que es fácil integrarlos en pequeños dispositivos. Por contra, un sensor de menor tamaño suele implicar que las muestras adquiridas poseen menor calidad, afectando a la precisión del reconocimiento. En otras ocasiones por el contrario, no es posible elegir entre un sensor grande o pequeño, como en la geometría de la mano. A veces, la seguridad física del sensor es importante para evitar ataques o intentos de destrucción, lo cual requiere refuerzos extra que tienen impacto en el tamaño y en el precio.

- Coste del sensor. Suele estar íntimamente relacionado con el tamaño, aunque también aparecen otros factores (por ejemplo, en iris es necesaria una óptica que permita capturar a distancias muy cortas y normalmente se usa iluminación infrarroja). Igualmente, hay que tener en cuenta que al coste del sensor hay que sumarle el resto de elementos necesarios a su alrededor: cableado, puesto de captura, mantenimiento, etc.

Otro atributo importante que está relacionado con un rasgo biométrico es el **tamaño de los datos digitales capturados** (en términos de decenas de bytes o megabytes). Ello afecta a la velocidad del canal de comunicación por el que han de viajar los datos biométricos, al tamaño que ocupa la base de datos con los patrones de los usuarios del sistema, y a la rapidez con la que es posible realizar el reconocimiento. Si el tamaño de los datos es lo suficientemente pequeño, puede hacerse uso de pequeñas tarjetas que almacenan los datos biométricos del usuario así como de dispositivos portátiles que usualmente tienen límites en su capacidad o velocidad de procesamiento (teléfonos móviles, PDAs, etc.). El tamaño de los datos que se manejan varía enormemente entre rasgos biométricos. Los rasgos que manejan imágenes (cara, huella, mano) pueden no obstante utilizar técnicas de compresión, reduciendo así su tamaño.

Por último, mencionar la **escalabilidad** de un rasgo como otro atributo importante para su elección. La escalabilidad hace referencia a la capacidad de un rasgo biométrico para identificar personas entre una gran población de sujetos sin que por ello el error o el tiempo de procesamiento se vean muy afectados. En parte tendrá que ver con el tamaño de los datos, pero también en gran medida con la precisión que un rasgo sea capaz de dar. Un rasgo poco escalable solamente será capaz de trabajar con bases de datos pequeñas, por lo que no podrá admitir más usuarios en el sistema. Los rasgos más escalables son la huella y el iris, mientras que la mano, cara y voz no lo son tanto. Por otro lado, en ocasiones la escalabilidad de un rasgo es un atributo no deseado porque puede presentar rechazo en su uso. Los rasgos escalables son los más usados en búsquedas de criminales, dado que suele trabajarse con bases de datos muy grandes que además, van aumentando a medida que se incorporan datos de nuevos criminales. Esta asociación puede hacer que un rasgo de este tipo no sea aceptado en aplicaciones comerciales del día a día, ya que por ejemplo los datos que se capturan de un empleado para acceder a un edificio podrían usarse sin su consentimiento para comprobar si su identidad se encuentra en una base de datos de criminales.

Factores que afectan a la aplicación

Si bien en el capítulo siguiente haremos una clasificación de las diferentes aplicaciones que hacen uso del reconocimiento biométrico, así como de sus particularidades, presentaremos aquí una serie de factores comunes a todas ellas que afectan a la hora de elegir un rasgo u otro:

- **Si los usuarios son cooperativos o no**. En aplicaciones donde un usuario conocido del sistema pretende obtener acceso, la cooperatividad será alta. Por contra, si lo que se pretende es comprobar si una persona está en una lista de criminales, el individuo será lo menos cooperativo posible. Los usuarios de aplicaciones cooperativas pueden utilizar tarjetas con sus datos biométricos, reduciendo así la capacidad de almacenamiento del sistema. Por el contrario, la única manera de identificar a usuarios no cooperativos es hacer una búsqueda sobre una base de datos completa que deberá estar centralizada en algún lugar.

- **Si el usuario es conocedor de que está siendo identificado o no**. En el segundo caso, necesariamente habré de usar un rasgo que pueda capturarse a distancia (cara, voz, etc.).

- **Si los usuarios están habituados al uso del sistema o no**. El uso de una aplicación de modo regular en el tiempo permitirá que los usuarios se habitúen al sistema. En otros casos, si el tiempo entre un uso y el siguiente es grande, el usuario perderá algo de destreza. Algunos rasgos o algunos tipos de sensores particulares (iris, huella, retina) pueden necesitar de un entrenamiento específico hasta que el usuario se habitúe a ellos. Otros sensores como las tabletas de firma no plantean tanta dificultad de uso, si bien el usuario puede extrañarse de tener que firmar sobre una pantalla donde antes firmaba sobre un papel.

- **Si la captura de datos es supervisada o no**. Las aplicaciones no cooperativas siempre serán supervisadas, mientras que las cooperativas pueden no serlo. En la mayoría de los sistemas, el registro del usuario suele hacerse de modo supervisado, aunque no siempre es necesario o posible. Por ejemplo, un usuario de banca on-line necesariamente deberá ir a una sucursal para registrarse en el sistema, pero más tarde podrá acceder a su cuenta desde su casa utilizando un sensor conectado a su ordenador.

- **El entorno y las condiciones donde operará el sistema**. No es lo mismo operar en una sala dentro de un edificio, donde la temperatura e iluminación pueden controlarse mejor, que en una instalación situada en la calle. Ello puede tener un fuerte impacto en la calidad de los datos adquiridos.

- **Si el uso del sistema es público o privado**. La actitud del usuario dependerá si el sistema va a usarse para acceder al edificio de su empresa (privado) o para pedir una ayuda social al estado (público). A su vez, también afectará que el rasgo biométrico implicado pueda usarse (fraudulentamente o no) para comprobar la identidad del usuario en otras bases de datos que pueda disponer la entidad administradora del sistema.

- **Si el sistema es abierto o cerrado**. Tiene que ver si el sistema va a necesitar, ahora o en el futuro, intercambiar datos con otros sistemas biométricos. Por ejemplo, entidades públicas que necesiten intercambiar datos con otras entidades de otros países. En este caso, es muy importante que la captura y almacenamiento de los datos siga algún estándar existente.

Capítulo 4

Aplicaciones y mercados del reconocimiento biométrico

4. Aplicaciones y mercados del reconocimiento biométrico

Al igual que los rasgos biométricos difieren en aspectos importantes, lo mismo sucede con las aplicaciones biométricas [53]. Éstas pueden diferir sustancialmente en factores como el nivel de seguridad requerido, la conveniencia para el usuario, el proceso de registro en el sistema o en el proceso de verificación de identidad. Usar el reconocimiento biométrico en aplicaciones de vigilancia o búsqueda de criminales, por ejemplo, es muy diferente a usarlo en el acceso a una red de ordenadores o al PC personal. En definitiva, para utilizar el reconocimiento biométrico de modo efectivo en una aplicación no sólo es necesario conocer las características de los rasgos biométricos, sino también las necesidades y particularidades de la misma. De la misma manera, junto con la variedad de aplicaciones de reconocimiento biométrico, existen una serie de mercados. Podemos hablar de una serie de aplicaciones *horizontales*, las cuales pueden ser usadas en distintos mercados *verticales*. El cuadro 1 muestra las distintas aplicaciones y mercados, así como su relación, la cual se comenta en los siguientes apartados.

4.1. Clasificación de aplicaciones y mercados

Se puede establecer los siguientes tipos de aplicaciones *horizontales* del reconocimiento biométrico [53]:

Aplicaciones de cara al ciudadano, dentro las cuales se engloban:

- **Identificación criminal** de un sospechoso o detenido.
- **Verificación de la identidad** en la interacción del ciudadano con servicios públicos como salud, voto, seguridad social, etc.
- **Vigilancia** de individuos presentes en un lugar en un momento determinado, por ejemplo en eventos públicos.

Aplicaciones de cara al empleado, dentro las cuales se engloban:

- **Acceso a equipos o redes**, sustituyendo o complementando los mecanismos tradicionales mediante clave.
- **Acceso físico a instalaciones**, típicamente a un edificio, en complemento o sustitución de llaves, tarjetas magnéticas, etc.

Aplicaciones de cara al cliente, dentro las cuales se engloban:

- **Comercio electrónico y transacciones remotas telefónicas**.
- **Terminales de punto de venta**, complementando o sustituyendo las tradicionales tarjetas con número PIN.

		MERCADOS				
APLICACIONES		Legal	Gubernam.	Financ.	Salud	Inmigrac.
Cara al ciudadadano	ID criminal	X				X
	Verif. Identidad		X			
	Vigilancia	X				X
Cara al empleado	Acceso PC/redes		X	X	X	
	Acceso físico	X	X	X	X	X
Cara al cliente	E-comerc. y transacc.					
	Punto de venta			X		

Cuadro 1. Relación entre aplicaciones y mercados del reconocimiento biométrico.

Igualmente, se establecen una serie de mercados *verticales* dentro de los cuales se engloban la mayor parte de las aplicaciones biométricas. Estos mercados verticales hacen uso de diversas aplicaciones, sin que una misma aplicación sufra importantes variaciones en los diferentes mercados. Por ejemplo, un control de acceso físico que haga uso de la mano funciona de modo más o menos parecido si se usa en un banco o en un aeropuerto. Los distintos mercados son:

- **Legal (forense),** que hace uso del reconocimiento biométrico para identificar a individuos sospechosos, detenidos, bajo situación de arresto o con restricciones de libertad (arresto domiciliario, etc.).

- **Gubernamental**, donde el reconocimiento biométrico se utiliza para controlar la interacción del ciudadano con entidades públicas y para la propia administración del sistema público.

- **Financiero**, al igual que el sector gubernamental, el reconocimiento biométrico controla la interacción del ciudadano con el sistema financiero (acceso a cuentas o transacciones comerciales) y la propia administración del sector, por ejemplo el acceso de empleados a redes protegidas.

- **Salud**, donde al igual que los dos casos anteriores, por un lado se controla la interacción del usuario (utilización de servicios sanitarios) y por otro lado se asegura el correcto funcionamiento del sistema (manejo de información médica por parte de empleados).

- **Inmigración**, donde el reconocimiento biométrico se usa para el control de movimientos a través de fronteras y para el control interno de los propios empleados dentro de las áreas restringidas de acceso.

4.2. Aplicaciones de cara al ciudadano

Como hemos visto, este tipo de aplicaciones incluyen la identificación criminal, la verificación de la identidad y la vigilancia. La componente más característica de todas ellas es que una institución gubernamental es la que requiere la comprobación de identidad. Por ello, las aplicaciones de cara al ciudadano tienen una mayor "obligatoriedad" de uso que otras aplicaciones biométricas, razón por la cual hay que prestar especial atención al respeto a la privacidad del usuario para evitar rechazo en su uso. Los datos biométricos y la comprobación de identidad suele hacerse de modo centralizado en un sistema operado por la propia institución gubernamental. El modo de funcionamiento a menudo es el de identificación (ver Sección 2.2) ya que puede haber necesidad de averiguar la identidad de un sujeto que no desea ser identificado o bien que intenta hacer uso de una identidad falsa. Ello tiene como inconvenientes el tiempo de procesamiento y el aumento de las tasas de error, al tener que comparar contra una base de datos de cientos o incluso millones de usuarios (hasta toda la población de un país).

La principal función del reconocimiento biométrico en la identificación criminal (biometría forense) es permitir el desarrollo de acciones legales contra un individuo. Esta función fue la primera donde el reconocimiento biométrico comenzó a utilizarse a gran escala, hace ya décadas. En este tipo de aplicación, la huella dactilar es el rasgo más usado (véase Cuadro

2) dado que lo primero que se captura de un criminal son sus huellas y dado que en una escena de un crimen lo más fácil de obtener son las huellas latentes. La cara y la voz también se utilizan para esta función, puesto que es usual conseguir fotos de criminales o intervenir sus llamadas, aunque la precisión que se consigue es menor que con la huella. Es posible que con el paso del tiempo se utilice el iris dada su alta fiabilidad, aunque el principal inconveniente es la inexistencia de bases de datos con el iris de criminales. Claramente, el principal mercado de la identificación criminal es el legal, aunque también tiene su hueco en el sector del control de inmigración.

		RASGOS						
APLICACIONES		Huella	Cara	Iris	Voz	Firma	Mano	Retina
Cara al ciudadadano	ID criminal	X	X	X	X			
	Verif. Identidad	X	X					
	Vigilancia		X		X			
Cara al empleado	Acceso PC/redes	X	X		X	X		
	Acceso físico	X		X			X	X
Cara al cliente	E-comerc. y transacc.	X	X		X			
	Punto de venta	X	X	X		X		

Cuadro 2. Rasgos más utilizados en las diferentes aplicaciones que hacen uso del reconocimiento biométrico.

En cuanto a la **verificación de la identidad**, el objetivo es comprobar la identidad de los individuos en su interacción con servicios públicos: voto, solicitud de beneficios sociales, expedición de documentos, uso del sistema de salud, etc. En este caso, el reconocimiento biométrico no sólo proporciona la identidad de un individuo, sino que permite evitar que una persona use varias identidades, que haga uso de servicios que no le corresponden suplantando otra identidad, etc. Un ejemplo de uso de esta aplicación es

el DNI electrónico, donde se almacenan los datos biométricos del individuo. El éxito de este tipo de aplicación vendrá dado a partir de que el usuario perciba que el uso del reconocimiento biométrico proporciona más seguridad en sus transacciones públicas, a la vez que se le garantice la privacidad de sus datos biométricos y que las instituciones no vayan a usarlos para otros fines que no sean puramente la verificación de identidad durante una transacción. Los rasgos más típicamente usados en estos casos son la huella y la cara, dada su implantación en los documentos de identidad tradicionales, y el uso de esta aplicación mayormente se produce en el sector gubernamental.

Por último, las aplicaciones de **vigilancia** pretenden comprobar la identidad de un individuo presente en un lugar en un momento determinado. Tras los atentados del 11-S del 2004 en las Torres Gemelas de Nueva York, el interés en este tipo de aplicación ha crecido enormemente, no sin controversia. Para ello, se contempla la colocación de cámaras en espacios públicos (aeropuertos, estadios, etc.) que monitoricen a las personas presentes y comprueben si entre ellas se encuentra algún criminal. Los principales escollos de esta aplicación son por un lado su rendimiento, puesto que no existe control sobre las personas en el momento de su captura, y por otro lado la posible invasión de privacidad. Resulta obvio que la cara es el rasgo más utilizado en esta aplicación, pudiendo contemplarse también la voz mediante la intervención de líneas telefónicas. El mercado con mayor implicación es el legal, seguido del de inmigración.

4.3. Aplicaciones de cara al empleado

Este tipo de aplicaciones incluyen el acceso a equipos o redes y el acceso físico a instalaciones. En este caso, su uso puede hacerse tanto por instituciones públicas como por empresas privadas, y su alcance no va más allá de un departamento, una empresa o una determinada institución. Estas aplicaciones pueden o no tener "obligatoriedad" y pueden llevarse a cabo bien a través de un sistema central, o bien proporcionando tarjetas individuales a los usuarios. En ellas, el modo de operación suele ser el de *verificación*, ya que el objetivo no es el de comprobar si una persona está en una lista, sino permitir el acceso a usuarios ya conocidos por el sistema. Su uso puede rebajar considerablemente los costes de una empresa al automatizar considerablemente el proceso de comprobación de identidad.

En el **acceso a equipos o redes**, el reconocimiento biométrico complementa o incluso sustituye los mecanismos tradicionales de claves. Hay un gran número de productos comerciales orientados a proporcionar soluciones de este tipo, dada la enorme difusión en el uso de ordenadores, dispositivos electrónicos portátiles, redes empresariales y acceso a Internet. Por un

lado, el reconocimiento biométrico proporciona conveniencia al usuario, que no tiene que recordar claves, y por otro proporciona seguridad en el acceso a datos o recursos sensibles. El rasgo más fuertemente asociado con esta aplicación es la huella, e incluso cada vez más dispositivos electrónicos incorporan pequeños sensores sin que el precio se vea repercutido de manera apreciable. Otros rasgos implicados son la cara y la voz, puesto que también existen sensores pequeños y baratos, pero su precisión de reconocimiento es menor, sobre todo por el hecho de que no siempre puede controlarse el entorno de uso (oficina, cafetería, aeropuerto, etc.). La firma es otro rasgo que está cobrando fuerza en esta aplicación debido a los nuevos dispositivos portátiles capaces de capturar escritura en la pantalla (teléfonos móviles, PDAs, etc.). Los mercados más importantes para esta aplicación son el financiero, salud y gubernamental, aunque en principio cualquier sector empresarial es susceptible de hacer uso de ella.

En cuanto al **acceso físico a instalaciones**, el objetivo es controlar la identidad de los individuos que acceden, salen o permanecen en un área, típicamente un edificio o una sala. El reconocimiento biométrico complementa o reemplaza a las llaves y tarjetas de identificación, y suele utilizarse en determinadas salas o instalaciones sensibles (militares, bancarias, etc.). Raramente se usa para controlar el acceso puerta por puerta, lo cual también despertaría rechazo en su uso. A su vez, evita que diferentes empleados compartan llaves o tarjetas, sin saber quién está accediendo en cada momento a la instalación, y también evita que una persona no autorizada pueda entrar robando las llaves o la tarjeta. Las modalidades más utilizadas son la huella y la mano. Esta última existe en multitud de instalaciones, mientras que la huella proporciona mayor precisión. Si se requiere muy alta seguridad en el acceso, se utiliza el iris o el escáner de retina. En cuanto a los mercados, el acceso físico a instalaciones puede utilizarse en prácticamente cualquier sector.

4.4. Aplicaciones de cara al cliente

Dentro de este tipo de aplicaciones encontramos el comercio electrónico y transacciones remotas telefónicas, y el uso en terminales de punto de venta. La principal característica de las mismas es que un proveedor de servicios o un vendedor es el que solicita la comprobación de identidad. La mayoría de las veces, el uso de éstas aplicaciones es opcional y al igual que las aplicaciones de cara al empleado, operan mayormente en modo verificación. A pesar de tratarse del tipo de aplicaciones que pueden dar mayor negocio al sector del reconocimiento biométrico, por el momento su desarrollo es el más reducido de todas las aplicaciones.

Las aplicaciones de **comercio electrónico** y **transacciones remotas telefónicas** engloban el uso del reconocimiento biométrico para la obtención remota de bienes o servicios. El reconocimiento biométrico complementa o replaza las tradicionales claves. Hasta el momento no hay un gran número de aplicaciones de comercio electrónico que hagan uso del reconocimiento biométrico. La mayor parte de los sistemas existentes son para transacciones remotas que usan la voz como método de comprobación de identidad. La necesidad de sistemas fiables y seguros de comprobación de identidad puede servir de revulsivo para el uso el reconocimiento biométrico en el comercio electrónico, para lo cual ayudará el creciente número de dispositivos que integran sensores pequeños y baratos (webcams, sensores de huella, etc.). En este sentido, los rasgos más usados podrían ser la huella y la cara. En las transacciones telefónicas, la voz es claramente dominante, aunque la huella puede emerger debido a los teléfonos móviles con sensores de huella integrados. Los sectores más involucrados en el uso de estas aplicaciones son el financiero (transacciones económicas) y el de salud (autorización de servicios médicos).

En cuanto al uso del reconocimiento biométrico en **terminales de punto de venta**, el objetivo es comprobar la identidad de personas para la obtención in situ de bienes o servicios. Al igual que el caso anterior, complementa o remplaza las tradicionales claves, tarjetas de crédito o firmas. La diferencia más clara, sin embargo, es que en este caso, el proceso está supervisado por el personal del punto de venta. La ventaja de esta aplicación es que el cliente está familiarizado con que se solicite comprobar su identidad en el momento de una venta, así como que el reconocimiento biométrico se percibe como más seguro que una tarjeta de crédito con firma o clave. Por el contrario, el reconocimiento biométrico puede percibirse como algo demasiado novedoso, lo cual puede producir un rechazo que inicialmente dificulte su uso. La firma se muestra como el rasgo más lógico, aunque una vez que las infraestructuras se desarrollen lo suficiente y se superen las reticencias iniciales de los usuarios, puede hacerse uso de otros rasgos como la huella, la cara, o incluso el iris para transacciones sensibles. El sector financiero es el más implicado en este tipo de aplicación.

Capítulo 5

Problemática actual y desafíos del reconocimiento biométrico

5. Problemática actual y desafíos del reconocimiento biométrico

5.1. Limitaciones de los sistemas biométricos

El hecho de que el reconocimiento biométrico esté extendido en múltiples sectores y aplicaciones no significa ni mucho menos que sea un problema totalmente resuelto [43, 44]. Aún hay margen de mejora en los sistemas biométricos, no solo desde el punto de vista de las tasas de error, sino también de la usabilidad de los sistemas y de su vulnerabilidad frente a ataques. A continuación detallamos algunas de las limitaciones de los sistemas biométricos que operan usando un solo rasgo. A pesar de que la tecnología va evolucionando y es capaz de aliviar algunos de estos, hay casos en los que resulta muy difícil ponerle solución.

Ruido en los datos adquiridos

Los datos capturados pueden estar perturbados o distorsionados [5]. Un dedo con cortes o quemaduras o la voz de una persona resfriada son un ejemplo. La perturbación también puede proceder de un mal mantenimiento del sensor (acumulación de suciedad) o de condiciones ambientales desfavorables (mala iluminación en caras, humedad en dedos, ruido de fondo en voz, etc.). El resultado es que los datos capturados no podrán ser correctamente comparados con otros datos, produciéndose errores. En ocasiones estos problemas pueden solucionarse tomando las medidas adecuadas (por ejemplo, limpiando el sensor), pero otras veces no es posible hacer nada (quemaduras en el dedo).

Variabilidad de los datos de un individuo

Los datos biométricos de un individuo no suelen ser iguales entre diferentes capturas, como puede verse en la Figura 13. A esta diferencia se la conoce como *variabilidad intraclase*. Esto sucede por ejemplo cuando el usuario interactúa de una manera distinta con el sensor cada vez que intenta usarlo (poniendo el dedo de distinta manera, firmando unas veces sentado y otras de pie, etc.). También sucede cuando se usan distintos sensores cada vez, lo que se conoce como interoperabilidad de sensores. En otros casos, el estado de ánimo o el simple paso del tiempo produce cambios en los rasgos, sobre todo en los rasgos de comportamiento (la voz cambia con la edad o la firma va evolucionando, por ejemplo). Todos estos factores tienen un claro efecto en las tasas de error, ya que el rasgo capturado puede ser muy diferente del modelo almacenado de ese usuario, incrementándose así el Falso Rechazo. Una solución a este problema consiste en ir actualizando el modelo almacenado del usuario a medida que pasa el tiempo.

Figura 13. Variabilidad intraclase: ejemplo de huellas de un mismo dedo.

Capacidad distintiva de los rasgos biométricos

Al igual que los datos biométricos de un individuo pueden variar con el tiempo, cabe pensar que en algún caso los datos de dos individuos distintos sean lo suficientemente parecidos como para no poder distinguirlos. Esto puede verse en la Figura 14. A este parecido se le conoce como *similitud interclase*. Este hecho también tiene su efecto en las tasas de error, incrementando la Falsa Aceptación. En la práctica no existe un rasgo biométrico para el cual los datos de cualquier par de individuos sean totalmente distintos, por lo que siempre hay un límite en términos de capacidad discriminativa.

No universalidad de los rasgos biométricos

Si bien se supone que cualquier individuo posee cualquier rasgo biométrico, en la práctica no es así. Por ejemplo, ciertos colectivos de población pueden no tener huellas adecuadas para el reconocimiento (trabajadores manuales). También puede suceder que por lesiones o accidentes, no se posea un rasgo biométrico de modo temporal o permanente (amputación de miembros, pérdida de voz, etc.). Como consecuencia, no es posible obtener un modelo fiable que represente la identidad del usuario, o directamente no es posible capturar el rasgo (Error de Fallo de Registro y Error de Fallo de Adquisición, respectivamente, ver Sección 2.3).

Figura 14. Similitud interclase: ejemplo de huellas de dedos distintos.

Ataques a sistemas biométricos

La seguridad de un sistema biométrico puede verse comprometida por ataques [35]. Podemos distinguir entre dos tipos de ataques:

- Ataques "esfuerzo cero" (en inglés, *zero-effort*), donde se aprovecha que la tasa de error nunca es cero, por lo que estadísticamente siempre habrá muestras de distintas personas lo bastante parecidas como para confundirlas (Falsa Aceptación mayor que cero).

- Ataques tipo "adversario" (en inglés, *adversary*), que se refiere a la posibilidad de que un impostor pueda hacerse pasar por otro individuo manipulando un rasgo biométrico o alguna parte del sistema de reconocimiento.

Los ataques "esfuerzo cero" hacen uso de la probabilidad de que dos muestras de distintas personas sean muy parecidas, lo cual es posible desde el punto de vista estadístico. Esta cuestión tiene que ver con la individualidad de un rasgo biométrico. La individualidad de un rasgo suele darse por supuesta, pero en la realidad es posible encontrarse con individuos que tienen rasgos muy parecidos, como en la Figura 14. Estadísticamente, si la Falsa Aceptación es del 1 % significa que uno de cada cien intentos de acceso fraudulento tendrá éxito. Para llevar a cabo este tipo de ataques, pueden usarse programas que sintetizan artificialmente rasgos biométricos, generando una gran cantidad de datos y ofreciéndoselos al sistema hasta

que se consiga entrar. Por ejemplo, para huella dactilar existe un software de generación de imágenes sintéticas de huellas, que puede encontrarse en *http://biolab.csr.unibo.it*

En cuanto a los ataques tipo "adversario", hay que considerar que los datos biométricos no son secretos. Una persona puede ser fotografiada, o sus huellas pueden obtenerse a partir de impresiones latentes dejadas al tocar objetos, y después estos datos pueden presentarse a un sistema para intentar acceder en nombre de esa persona. El tema de los ataques a sistemas biométricos está ahora mismo sobre la mesa y cada vez son más los estudios en los que se analiza la posibilidad de replicar rasgos y utilizarlos para pasar por esa persona (huellas de goma, fotografías de la cara o del iris, etc.) [35]. Aparte de esto, hay otros posibles ataques contra un sistema biométrico:

1. Vulnerar el sistema de reconocimiento con algún mecanismo informático o físico, de tal manera que se intercepten los datos que viajan por el mismo y se obtenga el control del mismo.

2. Repudio, donde un usuario legítimo puede cometer algún delito y después alegar que el sistema fue burlado por un intruso según el punto anterior o que le robaron su identidad (por ejemplo, un empleado de un banco con acceso a las cuentas de sus clientes).

3. Confabulación, en la cual un usuario con privilegios de administración sobre el sistema deliberadamente permite que un intruso acceda o tome el control.

4. Coacción, lo que sucede cuando un impostor fuerza a un usuario legítimo para que le permita acceder al sistema en su nombre.

5. Denegación de servicio, donde un atacante provoca que un sistema se colapse, de manera que los usuarios legítimos no puedan usarlo. Por ejemplo, pueden enviarse una serie de peticiones de acceso falsas muy seguidas, de tal manera que el sistema no sea capaz de atender todas y se bloquee. Otro ejemplo sería destruir físicamente el sensor.

Hay que notar que los ataques a sistemas biométricos no tienen que ver con la capacidad de reconocimiento de un rasgo biométrico, sino más bien con la operación del sistema y con los canales de comunicación que se utilizan. Por ejemplo, vulnerar el sistema por medios informáticos entra dentro del ámbito de la seguridad informática, no del reconocimiento biométrico. Para combatirlo, pueden usarse conexiones seguras y métodos de encriptación de datos. Hay que notar no todas las aplicaciones son

susceptibles de estos ataques. Por ello, a la hora de diseñar un sistema, hay que identificar cuales son las amenazas de ese sistema, quienes son los posibles atacantes, y cómo protegerse [14].

Multimodalidad biométrica

Algunas de las limitaciones de los sistemas biométricos que hemos visto en esta Sección pueden solventarse utilizando más de un rasgo biométrico para el reconocimiento, lo que da lugar a los llamados sistemas multimodales, ver Figura 15. Estos sistemas biométricos:

- son más precisos al combinar varios frentes de información.
- son más difíciles de suplantar al tener que atacar a varios rasgos.
- permiten cubrir mayor población que un sistema unimodal, puesto que es más difícil que un individuo no posea varios rasgos a la vez.

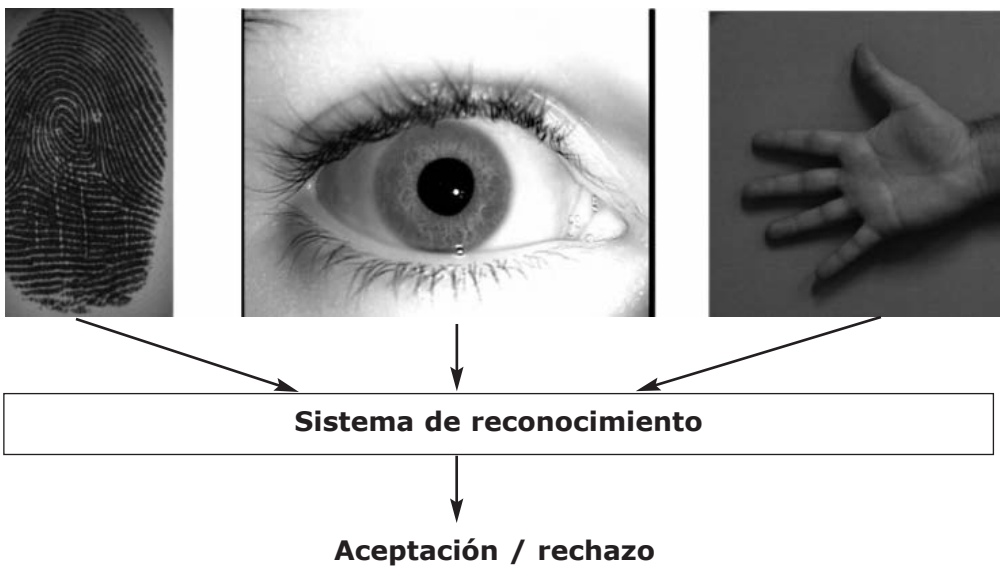


Figura 15. Combinación de varios rasgos en un sistema multimodal.

Un sistema multimodal puede operar de modos diferentes según el orden en el que se combinan las distintas fuentes de información, afectando de diferente manera al tiempo de respuesta y a la forma de interacción con el usuario:

- Modo serie: las salidas del análisis de un rasgo biométrico se usan como entrada para análisis del siguiente rasgo, reduciendo así en cada paso el número de identidades posibles antes de emplear la siguiente característica. Este modo se usa, por ejemplo, poniendo en primer lugar un sistema poco preciso pero de rápido procesado para después, una vez reducidas rápidamente las posibles identidades, emplear un sistema más preciso.

- Modo paralelo: la información de múltiples rasgos biométricos se emplea simultáneamente en el proceso de reconocimiento. En contraste al caso anterior, siempre se utilizan todos los sistemas fusionados lo cual a su vez requiere capturar todos los rasgos antes de decidir.

Por último, un sistema multimodal puede combinar información de múltiples fuentes según los siguientes esquemas:

- Múltiples sensores: se combina la información obtenida de diferentes sensores (con distinta tecnología o mecanismo de captura) para el mismo rasgo biométrico.

- Múltiples rasgos: se combinan diferentes rasgos biométricos como pueden ser la cara y la huella dactilar. Estos sistemas contendrán necesariamente más de un sensor, cada uno para un rasgo biométrico distinto.

- Múltiples instancias de un mismo rasgo: permite combinar las huellas dactilares de dos o más dedos de una persona, o una imagen de cada uno de los dos iris de un sujeto.

- Múltiples capturas de un mismo rasgo: se emplea más de una captura del mismo rasgo biométrico. Por ejemplo, se combinan múltiples impresiones del mismo dedo, múltiples muestras de voz o múltiples imágenes de la cara.

- Múltiples representaciones/comparaciones para un mismo rasgo: implica combinar diferentes enfoques para la extracción y comparación de las características biométricas.

Capítulo 6

Estándares biométricos

6. Estándares biométricos

En los últimos años ha habido una preocupación creciente por parte de las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante, aún la estandarización continua siendo deficiente y como resultado de ello, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietarios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor. Hablamos de un área tecnológica relativamente nueva, no consolidada, que ha dado lugar a múltiples estándares redundantes y no aceptados de forma única y global. No obstante, la industria biométrica está haciendo un esfuerzo importante para solucionar estos problemas, llegando cada vez más a un punto de convergencia, a la vez que se marca el camino a seguir en el futuro.

Son varios los elementos en los cuales dos sistemas biométricos pueden diferenciarse (recordemos la Figura 1): la forma de comunicarse con los sensores, el tipo de características y su forma de extracción, el mecanismo de comparar dos patrones distintos, el formato de almacenamiento de un modelo en la base de datos del sistema, etc. La no existencia de estándares hace que cada vendedor opte por una solución propietaria y que sus clientes queden "atados" a ellos cuando les compran un producto. Por otro lado, resulta complejo llegar a un consenso para estandarizar los sistemas biométricos, puesto que gran parte de los elementos que los forman (extracción de características, comparación de patrones, etc.) suelen constituir el "valor añadido" tecnológico que diferencia a los distintos fabricantes. En cualquier caso, cabe esperar que el desarrollo y uso de ciertos estándares permita optar por un mayor rango de dispositivos y tecnologías compatibles entre sí, sin poner en riesgo el *conocimiento* de las distintas empresas y a la vez facilitando el crecimiento del mercado.

6.1. Interfaces de Programación de Aplicaciones (API)

El estándar BioAPI

El consorcio BioAPI [11] nació en Abril de 1998 con el apoyo de algunas de las compañías informáticas más importantes (IBM, HP y Compaq) y en la actualidad tiene 163 miembros. Actualmente tiene dos especificaciones, la BioAPI 1.1 y la BioAPI 2.0. Es un estándar ampliamente aceptado por la industria biométrica y apoyado por agencias estatales como el caso de Estados Unidos.

De modo general, BioAPI intenta estandarizar el modo en que las aplicaciones se comunican con los dispositivos biométricos y la forma en que los datos son almacenados y utilizados. Sin embargo, no intenta estandarizar el modo en que los datos son generados por los dispositivos, ni en las características que cada fabricante extrae a partir de los rasgos biométricos. En este sentido, establece un alto nivel de abstracción que permite olvidar los detalles particulares de fabricación de cada producto y de las tecnologías empleadas.

El estándar BAPI

BAPI es un estándar desarrollado y patentado por una compañía, I/O Software, no por un consorcio de compañías e instituciones como en BioAPI. En el año 2000, Microsoft licenció este estándar, lo cual hizo que otras compañías como Intel lo adoptaran también.

Actualmente, el sector del reconocimiento biométrico se encuentra dividido entre BioAPI (considerado como estándar de facto por Estados Unidos para sus aplicaciones) y BAPI (apoyado por las dos grandes empresas Microsoft e Intel), dando lugar a una situación no deseada de confrontación entre dos estándares encaminados al mismo objetivo.

6.2. Formato de Ficheros Común para el Intercambio de datos Biométricos (CBEFF)

El estándar de Formato de Ficheros Común para el Intercambio Biométrico (*Common Biometric Exchange File Format* -CBEFF) [16] pretende definir los formatos de almacenamiento de los patrones generados a partir de los rasgos biométricos adquiridos, es decir, de las características extraídas. El objetivo es facilitar el acceso e intercambio de distintos tipos de datos biométricos entre sistemas o entre diferentes componentes de un mismo sistema, buscando un formato común para manejar los datos biométricos. Ello favorece la interoperabilidad entre aplicaciones, a la vez que simplifica la integración de sistemas y posibilita la compatibilidad de futuros sistemas con los presentes.

La primera versión de este estándar apareció en Enero de 2001 auspiciada por el Instituto Nacional de Estándares y Tecnología americano -NIST [54], y el Biometrics Consortium [10]. Una segunda versión revisada y aumentada apareció en Abril de 2004.

6.3. Seguridad biométrica -ANSI X9.84

El estándar ANSI X9.84, creado en 2001 por el ANSI (American National Standards Institute) [6] y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros, haciendo referencia a la transmisión y almacenamiento seguro de información biométrica así como a la seguridad e integridad del hardware asociado. Las necesidades particulares de esta industria han influido especialmente en la definición de estándares biométricos. Una organización acreditada por el ANSI, conocida como X9, que representa a bancos, uniones de crédito, organismos de regulación estatales, fabricantes, etc., es la responsable del desarrollo y publicación de los acuerdos alcanzados en materia de estándares para la industria financiera. Las actividades estandarizadoras afectan a tareas como la comprobación de procesos y transacciones, la gestión y protección de claves personales, el uso de técnicas criptográficas, los pagos a través de Internet, etc.

6.4. Principales organismos de estandarización

A nivel internacional encontramos los siguientes organismos coordinadores de actividades de estandarización biométrica, con más de 60 estándares en desarrollo:

- **Subcomité 37 (SC37) del Joint Technical Committee on Information Technology (JTC1) del International Organization for Standardization (ISO)**, lo cual se resume como ISO/IEC JTC1/SC37 [41]. El SC37 se estableció en Junio de 2002 y en él participan 24 Estados miembros, 6 países en calidad de observadores y 14 organizaciones. Hasta Abril de 2007, 16 estándares del SC37 han sido publicados como estándares internacionales ISO/IEC (incluyendo por ejemplo la participación en el desarrollo de BioAPI y CBEFF). El Subcomité 37 se ocupa de acciones como la interoperabilidad e intercambio de datos entre aplicaciones y sistemas, interfaces de comunicación, formato de ficheros y de datos para intercambio entre aplicaciones, metodologías de evaluación del rendimiento de sistemas biométricos así como de aspectos jurídicos y sociales acerca del uso de tecnologías biométricas. También mantiene una línea importante de trabajo acerca de la armonización del vocabulario biométrico.

- **Comité Técnico M1 del InterNational Committee for Information Technology Standards (INCITS)** [38], organismo acreditado por el American National Standards Institute (ANSI) [6]. El M1 fue establecido por el INCITS en Noviembre de 2001. Hasta Abril de 2007, 17 estándares han sido publicados como estándares

internacionales ANSI/INCITS, (incluyendo también la participación en el BioAPI y CBEFF). INCITS constituye el principal esfuerzo americano en la estandarización en el ámbito de las Tecnologías de la Información y las Comunicaciones, abarcando el almacenamiento, procesado, transferencia, gestión y recuperación de la información. INCITS M1 también participa en calidad de asesor dentro del JTC1/SC37 y es el representante de Estados Unidos en las reuniones del SC37.

- **Information Technology Laboratory (ITL) [55] del Instituto Nacional de Estándares y Tecnología americano (NIST)** [54], contribuidor importante a las actividades de estandarización de los organismos anteriores.

Existen además otros organismos internacionales impulsando iniciativas en materias biométricas tales como el **Biometrics Consortium** (BC) [10], el **International Biometrics Group** (IBG) [36], la **Biometrics Management Office** del Departamento de Defensa americano (DoD) [24] o el **European Biometrics Forum** (EBF) [26]. A nivel nacional, tenemos la **Agencia Española de Protección de Datos** (AEPD) [2], la **Asociación Española de Normalización y Certificación** (AENOR) [9], el **Centro Criptológico Nacional** (CCN) [17] y el **Instituto Nacional de Tecnologías de la Comunicación** (INTECO) [39].

Capítulo 7

Privacidad y aceptación social

7. Privacidad y aceptación social

7.1. Introducción

La actual aportación tecnológica de los sistemas de reconocimiento biométrico al sector de la seguridad, dentro de las aplicaciones propias de este tipo de sistemas, ha de venir sin duda acompañada de una evolución paralela en el ámbito de los derechos fundamentales de los usuarios en cuanto a temas de privacidad se refiere. Cabe destacar que el aspecto de desarrollo tecnológico, tanto lógico como físico, que se produce en el diseño y desarrollo de los sistemas de reconocimiento biométrico es un pilar fundamental para la integración de los mismos de manera efectiva dentro de los actuales sistemas de seguridad, pero no se puede olvidar por otro lado la necesidad de desarrollar otros aspectos "no técnicos". En la Figura 16 se puede observar la existencia mencionada de estos aspectos "no técnicos" y su relación con los aspectos más tecnológicos (técnicos) propios de estos sistemas.

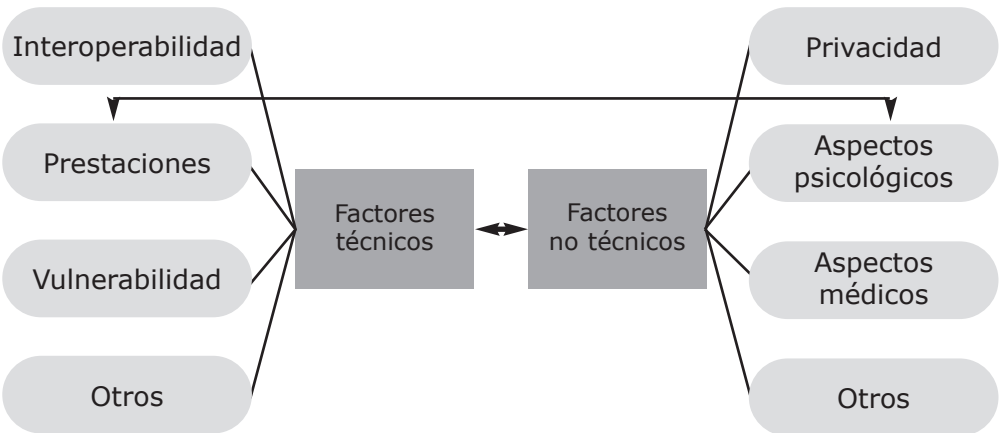


Figura 16. Relación entre aspectos técnicos y no técnicos de los sistemas biométricos. [25].

Aspectos tales como la aceptación por parte del usuario de las implicaciones de uso de este tipo de sistemas repercute directamente en las prestaciones que el sistema muestra en su funcionamiento, de ahí la línea de unión de la figura, atendiendo a la necesidad de colaboración de este usuario para su correcto funcionamiento.

Este punto resalta sin duda la existencia de aspectos relacionados con los sistemas de reconocimiento biométrico que tienen una relación directa con el respeto a la privacidad de los usuarios de los mismos. El claro ejemplo de sistemas que funcionan sin que el usuario tenga conciencia de ello, como aquellos en modo de vigilancia por ejemplo, tiene repercusiones sociales que es necesario resolver y administrar de manera eficaz para que no se presenten problemas que afecten a la implantación de los mismos, basando estas soluciones en el rol protagonista que tiene el usuario.

Estos aspectos no son en ningún caso algo novedoso en el desarrollo de nuevas tecnologías de seguridad y ya se presentaron años atrás en situaciones similares en las que era necesario hacer uso de datos personales de usuarios, como por ejemplo tras el desarrollo de la criptografía y de las PKI[1], lo que sin duda supuso un punto de inflexión en la política de privacidad de los Estados Unidos, ante la necesidad de garantizar el secreto de las claves de los usuarios de los nuevos sistemas de cifrado [46].

Todo este problema que aquí se plantea, hace necesaria una revisión de las políticas de gestión de datos y de la privacidad de los usuarios, y de las actuaciones que se llevan a cabo directamente relacionadas con los sistemas de reconocimiento biométrico, así como de las implicaciones de la gestión de datos personales de las bases de datos utilizadas en estos sistemas.

Tanto las políticas propias de los países como los tan necesarios estándares a nivel internacional, deben alzarse como garantes de estos derechos de privacidad al mismo tiempo que desarrollan las especificaciones técnicas igualmente necesarias.

Aunque quizás el problema más acusado en la definición de estas actuaciones en materia de privacidad, es precisamente la de definir claramente el horizonte que abarca la privacidad y sus implicaciones en cuanto al uso de datos en los sistemas biométricos y otros sistemas automatizados de gestión de datos personales.

Atendiendo a su significado semántico, la definición de la Real Academia de la Lengua de privacidad es: "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". En este sentido, la definición semántica de la palabra, no difiere en exceso de las que se pueden encontrar en otras lenguas, pero sin embargo el carácter puramente subjetivo de esta noción, dota a la definición de este aspecto de matices propios de cada persona, dependiente en todo caso de los condicionantes sociales

[1] PKI: Public Key Infraestructure

circundantes. Por tanto, juega un papel fundamental la confianza de las personas en las instituciones y organismos que gestionan sus datos personales y el uso que de ellos se hace con el objetivo de desarrollar los sistemas de seguridad, así como de la percepción de seguridad que estos sistemas aporten a cada persona, en función de los datos personales que esta haya tenido que proporcionar.

Podríamos hablar aquí de un trueque "privacidad-seguridad", influenciado en todo caso por el entorno actual, y la falta de seguridad latente en la sociedad, a partir de los diversos acontecimientos ocurridos en los últimos años, y que sin duda han servido como detonante para observar la importancia, tanto de desarrollar mejores sistemas y políticas de seguridad, como de afianzar la confianza de la gente en la necesidad de colaborar y participar en el desarrollo de estos.

7.2. Políticas de gestión de la privacidad

La intención a nivel europeo de generar políticas de seguridad de carácter general, contribuyendo así a la creación de un espacio europeo de seguridad común, requiere sin duda un exhaustivo y minucioso trabajo en diversos aspectos relacionados con la seguridad, y lógicamente la protección de la privacidad de los datos personales es un aspecto que repercute notablemente en que estas mismas políticas de seguridad calen en la sociedad.

Una primera aproximación a las políticas de protección de datos, a nivel europeo, se realizó en 1981, y se describe en "*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*" [29], en la que se lleva a cabo una primera aproximación para definir las necesidades de protección de los datos personales en los emergentes (por aquel entonces) sistemas de procesado de este tipo de información. Uno de los apartados principales de este tratado es la incorporación de las definiciones necesarias dentro del ámbito de la privacidad de datos, tales como la de datos personales, refiriéndose a "cualquier información relativa a un individuo identificado o identificable", así igual que la de procesado automático, como el "proceso que incluye las siguientes operaciones llevadas a cabo mediante medios automatizados de manera total o parcial: almacenamiento de datos, realización de operaciones tanto lógicas como aritméticas en estos datos, alteración, borrado, recuperación o diseminación de los mismos", lo que incluye sin duda el reconocimiento biométrico.

La Directiva 95/46/CE [23], del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo

que respecta al tratamiento de datos personales y a la libre circulación de estos datos, constituye el texto de referencia, a escala europea, en materia de protección de datos personales. En esta directiva se crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea, fijando límites estrictos para la recogida y utilización de los datos personales y solicitando la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

Así por ejemplo en España encontramos la Agencia Española de Protección de Datos [2], o en Francia la Commission Nationale de l'Informatique et des Libertés (CNIL) [19], una de las más prolíficas en cuanto a los trabajos relacionados con el ámbito del reconocimiento biométrico, y que además cuenta con otros organismos de apoyo tales como el Comité Consultatif National d'Ethique (CCNE) [18, 57], en la difícil tarea de observar este sector tecnológico de la biometría, que contempla un desarrollo mucho mayor en este país, al igual que en otros como Estados Unidos, Japón o Alemania y que dista mucho del que se observa en la actualidad en España.

Posteriormente en agosto de 2005, se llevó a cabo un informe acerca de los progresos en la aplicación de esta directiva (nº 108), en relación a la recolección y procesado de datos biométricos [20], en el que primeramente se definen una serie de ámbitos tales como: sector policial, empleo de personas, gestión de datos personales en el Sector Público, datos médicos, videovigilancia, tarjetas inteligentes y PIN (*Personal Identification Numbers*), en los que los progresos en el ámbito de la protección de datos referente a los sistemas biométricos pueden resultar de significante importancia. En el último apartado de este informe y tras revisar aspectos básicos del desarrollo de sistemas biométricos, se lleva a cabo un análisis de aquellos aspectos en los que se relaciona la protección de datos con el uso de sistemas de este tipo.

Anteriormente el *Data Protection Working Party*, adoptó el 1 de agosto de 2003, un documento de trabajo [8] en el ámbito de la biometría, precisamente en el cual se basa el informe [20].

En todo caso, dada la creciente globalización actual y el flujo continuo de datos, se han tomado iniciativas a nivel europeo desde la Comisión Europea de Libertad, Seguridad y Justicia, donde se trata con especial importancia el apartado de Protección de Datos [21].

A nivel nacional, como ya se ha indicado anteriormente, la Agencia Española de Protección de Datos [2], al amparo del artículo 18.4 de la Constitución Española, que establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos», es el órgano encargado de garantizar el cumplimiento de las políticas de protección de datos, existiendo además otras agencias de carácter autonómico en la Comunidad de Madrid [3], Cataluña [1] y el País Vasco [4]. Estas políticas vienen definidas en la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, abreviada como LOPD [47], que tiene por objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar".

Como antecedentes normativos a esta ley encontramos el ya citado artículo 18.4 de la Constitución Española, la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal de 26 de Octubre (LORTAD) [48], y la Directiva Europea 95/46 CE [23].

En relación a esta normativa podemos encontrar dos puntos importantes:

- El Real Decreto 994/1999 de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal de 11 de Junio de 1999 (RMS) [70] (que quedará derogado a partir del 19/04/2008): Es un reglamento que desarrolla la LORTAD, regula las medidas técnicas y organizativas que deben aplicarse a los sistemas de información en los cuales se traten datos de carácter personal de forma automatizada.

- El Real Decreto 1720/2007 [71], aprobado en Consejo de Ministros el 21 de Diciembre de 2007, de desarrollo de la LOPD, publicado en el BOE el 19/01/2008, y que entrará en vigor el próximo 19/04/2008. Se trata de un desarrollo de la Ley Orgánica 15/99, en cuanto a los principios de la ley, y a las medidas de seguridad a aplicar en los sistemas de información.

Este último punto sin duda marcará las futuras medidas en este ámbito.

7.3. Otras iniciativas a nivel europeo

Está claro que en una sociedad como la actual, en la que el aspecto tecnológico tiene un papel fundamental, el control de los condicionantes propios de esta misma tecnología se antoja necesario para evitar problemas

que afecten directamente a los propios usuarios, destinatarios últimos de esta tecnología, que deben percibir este tipo de avances como una mejora que no repercuta negativamente en modo alguno a ningún aspecto de su vida.

Así diversos apartados como los relacionados con el reconocimiento de personas en todas sus diversas posibilidades de presentación, y en general de la gestión de identidades, es un aspecto que día a día cobra mayor relevancia, y más si atendemos a la creciente proliferación de negocios y mercados que basan su correcto funcionamiento y evolución en la confianza en que es necesario llevar a cabo sus procesos, como son por ejemplo la banca y el comercio electrónico, y que sin duda se ven inversamente perjudicados por la desconfianza que se genera a diario, y que supone una mayor inseguridad en el centro de estos negocios que es el propio usuario.

Lo que supone este aspecto a nivel europeo es sin duda la concienciación de los máximos responsables de que es necesario llevar a cabo iniciativas en este sentido para paliar los posibles motivos de inseguridad que puedan aparecer. Esto sin duda se refleja claramente en la aparición de una nueva prioridad en el Programa Marco de I+D (*Framework Program*), en los que se pueden encontrar iniciativas como la red de excelencia FIDIS (*Future of IDentity in the Information Society*) [30], aunque en este caso perteneciese al pasado FP6, pero que sin duda en este nuevo FP7 supondría el nexo de unión entre las prioridades de seguridad (tema 10) y las relativas a las tecnologías de la información y las comunicaciones (tema 3). En este caso, FIDIS trata de resolver el problema que el incremento de sistemas que gestionan la identidad de la gente supone a la hora de tratar una información tan delicada, y que afecta a multitud de aspectos como la accesibilidad, la movilidad, etc.

Desde 1998 hasta 2003, la Comisión Europea, ha financiado 28 proyectos de investigación sobre biometría, en el ámbito de sus diversos programas relativos a las TICs (Tecnologías de la Información y las Comunicaciones). En la mayoría de ellos, se resalta la necesidad de llevar a cabo investigación en el campo de la ética de las implicaciones biomédicas de la biometría.

Una iniciativa que sin duda abarca esta cuestión es el proyecto BITE (*Biometric Identification Technology Ethics*) [12], financiado por la Comisión Europea, y que trata de dar pie a un debate público acerca del aspecto bioético inherente a la tecnología biométrica, basado principalmente en el crecimiento de dispositivos dedicados a tal efecto, el cual se prevé siga en aumento, y que requiere de acciones en tal sentido para controlar aspectos sociales, no controlables desde las empresas que desarrollan los

algoritmos y dispositivos de tales sistemas, pero que sin duda afectan al buen funcionamiento futuro del sector.

El proyecto está basado por tanto, en las diversas inquietudes de carácter social, legal y éticas, basadas en una amplia variedad de factores, que incluyen, entre otros, el miedo a la centralización de los datos relativos a la identificación biométrica, y el uso incorrecto de estos.

Las competencias del proyecto BITE son:

1. Definir y considerar los diversos aspectos bioéticos, que surgen del desarrollo y uso de las tecnologías de identificación biométrica emergentes.

2. Analizar el actual campo de investigación, en particular, para repasar:

   - La pruebas que evidencian la importancia del uso de las tecnologías de identificación biométrica para fines de seguridad en el campo biomédico.

   - Evidenciar, igualmente, la importancia de adoptar estas tecnologías para evitar el uso ilícito de ayudas médicas y sociales.

   - Las bases, para relanzar el uso de tecnologías biométricas como fuente de información biomédica de las personas.

3. Considerar las aplicaciones potenciales de las tecnologías de identificación biométrica, y el riesgo de hacer mal uso tanto de sus funciones como de la información relativa a estos sistemas.

4. Considerar:

   - La ética relativa a la "informatización del cuerpo" [69].

   - Las implicaciones éticas de la aplicación de la biometría para verificar y autenticar identidades en el sector médico y de asuntos sociales.

   - El impacto ético del uso de tecnologías biométricas en grupos vulnerables (niños, gente con problemas psicológicos, inmigrantes,…).

   - El impacto, en líneas generales, de la biometría en aquellas personas con características físicas relevantes y necesidades especiales.

7.4. Conclusiones

El objetivo de este capítulo, era el de dar a entender la necesidad de mantener en equilibrio la balanza del aspecto tecnológico y del cumplimiento de los principios éticos y morales que sin duda conlleva la utilización de las, cada día, más avanzadas tecnologías. Como ha ocurrido en otros muchos casos es necesario desarrollar marcos normativos que permitan determinar los pasos a seguir para el cumplimiento de los derechos fundamentales del usuario, más allá de los estándares y guías de fabricación de tecnologías que indudablemente son también importantes para el correcto desarrollo de todo sector.

La sociedad es la que determina el éxito de los sistemas de identificación basados en rasgos biométricos. Por ejemplo, las tecnologías que requieren muy poca cooperación o participación de los usuarios suelen ser percibidas como más convenientes, pero por otro lado éstos pueden ser capturados sin darse cuenta y esto es percibido como una amenaza a la privacidad por parte de muchos usuarios. Asimismo, el mero hecho de que se verifique la identidad de un individuo deja un rastro de información privada. Pero el tema de la privacidad adquiere más relevancia con los sistemas de reconocimiento biométrico porque los rasgos biométricos pueden proporcionar información adicional de un individuo, como afecciones médicas. Aún más importante, la gente puede sentir temor de que sus datos biométricos se enlacen de unos sistemas a otros, incluso sin su consentimiento. Así, el éxito de estos sistemas no vendrá dado hasta que los agentes implicados aseguren a los usuarios que sus datos biométricos se mantendrán seguros y no se usarán para otro propósito que el de la operación del propio sistema. En este sentido, es necesaria una legislación por parte de las autoridades que asegure que dicha información debe ser privada y que su uso fraudulento sea castigado.

Para ello es necesario afrontar ciertos aspectos fundamentales relacionados con este problema, tales como:

- Revisar las evidencias científicas de la biometría con particular hincapié en lo referente a la privacidad.

- Revisar la implementación de las leyes y políticas existentes al respecto, y hacerlas evolucionar en función de las necesidades existentes.

- Desarrollar estrategias que permitan implementar modelos de futuro, mediante los cuales se puedan anticipar los problemas más importantes en lo concerniente a la biometría y la privacidad,

aportando igualmente métodos de alerta temprana para anticipar la aparición de nuevas cuestiones éticas, sociales y legales, en lo referente a la tecnología y al sector en general.

Todas estas líneas de actuación tiene como objetivo prioritario actuar sobre cuestiones e incógnitas planteadas en torno a esta tecnología, y tratar de encontrar la respuesta a incertidumbres tales como:

- ¿Es el uso de los sistemas biométricos compatible con la privacidad de cada persona?
- ¿Permitirá la biometría tener un espectro simultáneo de visión de estos dos aspectos tan críticos?
- ¿Puede garantizarse la privacidad, a aquellas personas que son más reacias a dar su consentimiento hacia el uso de la biometría?
- ¿Pueden los patrones biométricos estar relacionados con características de comportamiento, o predisposiciones médicas?
- ¿Bajo qué condiciones puede hacer mal uso la información biométrica?
- ¿En qué situaciones, pueden los potenciales riesgos del uso de la biometría ser mayores que los beneficios?
- Retos actuales y políticas de presente y futuro a seguir.

Como apunte final es necesario señalar que una valoración poco apropiada de las normativas vigentes, y de las cuestiones e incógnitas relativas a estas implicaciones éticas que rodean a los sistemas de reconocimiento biométrico, pueden acarrear consecuencias graves, llegando incluso a provocar problemas en la implantación de la tecnología biométrica como referente de los sistemas de reconocimiento de personas y de los sistemas de seguridad.

Capítulo 8

Catálogo de empresas de biométrica

8. Catálogo de empresas de biometría

8.1. Empresas nacionales

Existe un número importante de empresas españolas dedicadas a la biometría. Entre ellas encontramos empresas cuya actividad va más allá, abarcando un espectro de actividad mucho mayor y proporcionando soluciones tecnológicas de muchos tipos (por ejemplo, Indra S.A. o Telefónica I+D). En los últimos años, no obstante, han aparecido un número de ellas dedicadas exclusivamente a la seguridad y/o a la biometría, siendo éstos los núcleos principales de su actividad. A continuación se ofrece un listado detallado con información de contacto.

Agnitio SL.

- URL: www.agnitio.es
- E-mail: info@agnitio.es
- Dirección: c/ Virgilio 25, Ciudad de la Imagen, 28223 Pozuelo de Alarcón, Madrid
- Rasgos: voz, firma on-line, multimodalidad biométrica

Biometric Technologies SL.

- URL: www.biometco.com
- E-mail:
- Dirección: C/ Diputación, 238, 1-4, 08007 Barcelona
- Rasgos: huella, voz, cara, multimodalidad biométrica

ETRA Investigación y Desarrollo, S.A.

- URL: www.etra.es
- E-mail:
- Dirección: C/ Tres Forques, 147, 46014 Valencia
- Rasgos: firma off-line

Indra S.A.

- URL: www.indra.es
- E-mail:
- Dirección: C/ Velázquez, 132, 28006 Madrid

Ingeniería de Sistemas para la Defensa de España (ISDEFE)

- URL: www.isdefe.es
- E-mail: general@isdefe.es
- Dirección: C/ Edison 4, 28006 Madrid
- Actividades: apoyo técnico de ingeniería y servicios de consultoría en tecnologías avanzadas, tanto en el sector de defensa como en el civil

Instituto Nacional de Tecnologías de la Comunicación (INTECO)

- URL: www.inteco.es
- E-mail:
- Dirección: C/ Moisés de León, 57, Edificio Bordadores II - 24006 León
- Actividades: investigación aplicada, impulso tecnológico, Centro de Alerta Temprana de Virus (CATA), observatorio de seguridad de la información, formación

Intuate Biometrics

- URL: www.intuate.com
- E-mail: comercial@intuate.com
- Dirección: C/ Aribau, 171, 1. 1a, 08036 Barcelona
- Rasgos: huella, iris, cara

Kimaldi Electronics

- URL: www.kimaldi.com
- E-mail: kimaldi@kimaldi.com
- Dirección: Ctra. de Rubí, 292 B, Pol. Ind. Can Guitard, 08220 Terrassa (Barcelona)
- Rasgos: huella

Centro Tecnológico ROBOTIKER

- URL: www.robotiker.com
- E-mail:
- Dirección: Parque Tecnológico, Edif. 202, 48170 Zamudio (Vizcaya)
- Rasgos: huella, cara, iris, mano, multimodalidad biométrica

SAB, Sociedad Avanzada de Biometría

- URL: www.sabiometria.net
- E-mail:
- Dirección: Edificio CEEI, Avda. Benjamin Franklin 12, 46980 Parc Tecnologic, Paterna (Valencia)
- Rasgos: huella, iris, retina

SeMarket

- URL: www.semarket.com
- E-mail:
- Dirección: Diputación, 238, 08007 Barcelona
- Rasgos: voz, huella, cara

SHS Consultores

- URL: www.shsconsultores.es
- E-mail: shs@shsconsultores.com
- Dirección: Edif. SHS Iris I, C/ Max Planck s/n, 41092 Isla de la Cartuja (Sevilla)
- Rasgos: iris

TAGRV, S.L. (PARC BIT)

- URL: www.tagrv.com
- E-mail: tagrv@tagrv.com
- Dirección: Parc Bit, Edifici 17 - Mòdul C8, Crta. de Valldemossa km.7,4 - 07121 - Palma - Baleares
- Rasgos: huella, voz, cara, multimodalidad biométrica

TB-Security

- URL: www.tb-security.com
- E-mail: comercial@tb-security.com
- Dirección: C/Marqués de Cubas, 25 6º Izq.- 28014 Madrid
- Rasgos: análisis forense, seguridad informática

TEUSS

- URL: www.teuss.com
- E-mail: info@teuss.com
- Dirección: C/ Viladomat, 192, 08029 Barcelona
- Rasgos: huella, cara, iris

Telefónica Investigación y Desarrollo, S.A.U.

- URL: www.tid.es
- E-mail: www@tid.es
- Dirección: C/ Ocata, 1, 08005 Barcelona
- Rasgos: voz

8.2. Empresas internacionales

Dado el gran número de empresas internacionales, se muestra a continuación una lista solamente con el nombre de cada una agrupadas por rasgo biométrico. Puede encontrarse más información de las mismas en [76].

HUELLA DACTILAR

- 123ID, Inc.
- ActivCard
- Artemis Solutions Group LLC
- Astro Datensysteme AG
- Atmel FingerChip Sensors
- AuthenTec, Inc .
- Axxis Biometrics, LLC
- BDC Consultancy Services
- BERGDATA USA, Inc.

- BIO-key International
- BioLink Technologies
- Biometric Access Corporation (BAC)
- Biometrics.co.za
- BiometriKa
- BiometriX Int.
- BioPay
- Bioscrypt, Inc.
- BKS
- Cansec Systems,Ltd.
- Cogent Systems
- Cross Match Technologies, Inc
- Cryptometrics
- Datastrip
- DERMALOG
- Digent
- Digital Persona
- East Shore Technologies
- Ethentica, Inc.
- Fingerprint Cards
- FingerPrint USA Consulting
- Fujitsu Microelectronics of America
- Global Integrated Software Solutions, Inc. (BioFirst)
- GREEN BIT srl
- Guardware Systems, Ltd.
- Harris Criminal Justice Products
- Heimann Biometric Systems
- I/O Software
- id3 Semiconductors
- IDENCOM Germany GmbH
- Identix
- IDLink Systems Pte Ltd.
- Infineon Technologies AG

- Innovatrics
- Integrated Biometric Technology
- IQS Biometric Solutions
- Keytronic
- Kimaldi
- Labcal Technologies
- LaserCard Systems
- Mitretek Systems
- Motorola Semiconductor Products
- NEC
- NITGEN
- Pantech
- Pen-One
- Precise Biometrics
- PrintScan
- Ringdale
- SAFLINK Corp.
- SAGEM MORPHO, Inc.
- SecuGen Corporation
- Sense Technologies
- Smart Biometrics
- Sony Startek Engineering
- STMicroelectronics
- Suprema, Inc.
- TBS North America
- TechSense Ventures Group
- Testech
- TSSI, Ltd
- Ultra-Scan Corporation
- Unisys
- Uvix Corporation
- Veridicom
- VeriTouch, Ltd.

- Zvetco

CARA

- 3dMD
- A4Vision
- AcSys Biometrics
- Animetrics
- Attrasoft
- Aurora Ltd.
- AWT
- Biometrica Systems
- BIOVISEC
- Cognitec Systems GmbH
- C-VIS Computer Vision and Automation GmbH
- CyberExtruder
- Cryptometrics
- FACE Technologies (PTY) Ltd.
- FIRSTEC
- Genex Technologies, Inc.
- Geometrix
- IdentAlink Ltd.
- Identix
- Image-Metrics, Ltd.
- MIT Media Laboratory Vision Modeling Group
- Neurodynamics
- Neven Vision
- Ringdale
- Sintec Co., Ltd.
- SpotIt
- Titanium Technology Ltd.
- Videology
- Viisage Technology
- Visphore

VOZ

- Authenfity
- BBN Speaker Recognition
- Diaphonics, Inc.
- General Masters/Saflink
- IBM Conversational Biometrics Group
- Inter Voice -Brite
- Keyware Technologies
- Microsoft Speech Server
- Neusciences
- NewFound Technologies
- Nuance
- Recognition Technologies, Inc
- ScanSoft
- SecuriVox
- Sensory
- Sonetech Corporation (TACSCAN)
- T-NETIX's SpeakEZ Voice Print Speaker Verification
- VeriTouch, Ltd.
- VeriVoice
- Voice Security Systems, Inc.
- VoiceMatch
- VoiceVantage LLC
- Voicevault

IRIS

- Alpha Engineering
- Evermedia
- HumanScan GmbH
- Iridian Technologies
- Iritech
- JIRIS
- LG Electronics: Iris Technology Division

- Neurotechnologija
- OKI America
- Panasonic
- Sarnoff Corporation
- SecuriMetrics PIER Handheld Iris
- Senex technologies
- Smart Sensors Ltd.

ESCRITURA Y FIRMA

- Cyber SIGN Inc.
- Communication Intelligence Corporation
- DynaSig
- SMARTpen
- Softpro SignPlus
- Valyd, Inc.
- WACOM
- WonderNet, Ltd.

MANO

- BioMet Partners
- Recognition Systems
- DERMALOG

RETINA

- Retica Systems, Inc.

Capítulo 9

Grupos de I + D

9. Grupos de I+D

9.1. Universidades españolas

Grupo de Reconocimiento Biométrico (ATVS)
Universidad Autónoma de Madrid

- URL: http://atvs.ii.uam.es
- E-mail: atvs@uam.es
- Dirección: Escuela Politécnica Superior, Campus de Cantoblanco, Universidad Autónoma de Madrid
- Rasgos: huella, voz, firma, escritura, iris, mano, multimodalidad biométrica

Grupo de Procesado de Voz (AHOLAB)
Universidad del País Vasco

- URL: http://bips.bi.ehu.es
- E-mail: aholab@bips.bi.ehu.es
- Dirección: Escuela Técnica Superior de Ingeniería de Bilbao
- Rasgos: voz, firma, multimodalidad biométrica

Diseño Microelectrónico y Aplicaciones
Grupo Universitario de Tarjeta Inteligente (DMA-GUTI)
Universidad Carlos III de Madrid

- URL: www.uc3m.es/uc3m/dpto/IN/dpin08/guti/iindex.html
- E-mail:
- Dirección: Universidad Carlos III de Madrid, Campus de Leganés
- Rasgos: huella, cara, iris, mano, firma, multimodalidad biométrica

Face Recognition and Artificial Vision Group (FRAV)
Universidad Rey Juan Carlos de Madrid

- URL: http://frav.escet.urjc.es
- E-mail:
- Dirección: Universidad Rey Juan Carlos, Campus de Móstoles, Madrid
- Rasgos: cara, multimodalidad biométrica

Grupo de Algorítmica aplicada a la Visión Artificial y a la Biometría (GAVAB)
Universidad Rey Juan Carlos de Madrid

- URL: http://gavab.escet.urjc.es
- E-mail:
- Dirección: Universidad Rey Juan Carlos, Campus de Móstoles, Madrid
- Rasgos: cara, firma, multimodalidad biométrica

Grupo de Aplicaciones del Procesado de Señales (GAPS)
Universidad Politécnica de Madrid

- URL: www.gaps.ssr.upm.es
- E-mail: gaps@gaps.ssr.upm.es
- Dirección: Departamento de Señales, Sistemas y Radiocomunicaciones, Escuela Técnica Superior de Ingenieros de Telecomunicación, Universidad Politécnica de Madrid
- Rasgos: voz

Grupo de Biometría y Tratamiento Numérico de la Información (GBTNI)
Universidad Politécnica de Madrid

- URL: www.mat.upm.es
- E-mail: www@mat.upm.es
- Dirección: Departamento de Matemática Aplicada a las Tecnologías de la Información, Escuela Técnica Superior de Ingenieros de Telecomunicación, Universidad Politécnica de Madrid
- Rasgos: iris

Grupo de Procesado Digital de Señales (GPDS)
Universidad de Las Palmas de Gran Canaria

- URL: www.gpds.ulpgc.es
- E-mail: gpds@gi.ulpgc.es
- Dirección: Departamento de Señales y Comunicaciones, Universidad de Las Palmas de Gran Canaria, Campus de Tafira
- Rasgos: cara, mano, firma, multimodalidad biométrica

Grupo de Reconocimiento de Patrones (GREPA)
Universidad de Salamanca

- URL: http://encina.fis.usal.es/~lalonso
- E-mail:
- Dirección: Departamento de Informática y Automática, Facultad de Ciencias, Universidad de Salamanca
- Rasgos: huella, voz

Grupo de Tecnología del Habla (GTH)
Universidad Politécnica de Madrid

- URL: www-gth.die.upm.es
- E-mail:
- Dirección: Escuela Técnica Superior de Ingenieros de Telecomunicación, Universidad Politécnica de Madrid
- Rasgos: voz

Grupo de Tratamiento de Señal
Escuela Universitaria Politécnica de Mataró (GTS-EUPMt)

Universidad Politécnica de Cataluña

- URL: www.eupmt.es/veu
- E-mail:
- Dirección: Escuela Universitaria Politécnica de Mataró
- Rasgos: huella, voz, cara, iris, mano, firma, multimodalidad biométrica

Grupo de Teoría de la Señal (GTS)
Universidad de Vigo

- URL: www.gts.tsc.uvigo.es
- E-mail:
- Dirección: Departamento de Teoría de la Señal y Comunicaciones, ETSI de Telecomunicación. Campus universitario Vigo, 36310 Vigo (Pontevedra)
- Rasgos: voz, cara, multimodalidad biométrica

Human Computer Technology Lab (HCTLab)
Universidad Autónoma de Madrid

- URL: www.hctlab.com
- E-mail:
- Dirección: Escuela Politécnica Superior, Campus de Cantoblanco, Universidad Autónoma de Madrid
- Rasgos: voz

Instituto de Investigación en Ingeniería de Aragón (I3A)
Universidad de Zaragoza

- URL: http://i3a.unizar.es
- E-mail: i3a@unizar.es
- Dirección: Instituto de Investigación en Ingeniería de Aragón
- Rasgos: voz, cara, mano, multimodalidad biométrica

Pattern Recognition and Human Language Technology Group (PRHLT)
Instituto Tecnológico de Informática (ITI)
Universidad Politécnica de Valencia

- URL: http://prhlt.iti.es
- E-mail:
- Dirección: Ciudad Politécnica de la Innovación, Camino de Vera s/n, 46022 Valencia
- Rasgos: voz, huella

Reconocimiento de Imágenes y Visión Artificial (RIVA)
Instituto Tecnológico de Informática (ITI)
Universidad Politécnica de Valencia

- URL: www.iti.upv.es/groups/riva
- E-mail: iti@iti.upv.es
- Dirección: Ciudad Politécnica de la Innovación, Valencia
- Rasgos: huella, voz, cara, multimodalidad biométrica

SINTONÍA
Universidad Carlos III de Madrid

- URL: www.uc3m.es
- E-mail:
- Dirección: Departamento de Informática, Universidad Carlos III de Madrid, Campus de Leganés
- Rasgos: voz, cara, multimodalidad biométrica

Centro de Tecnologías y Aplicaciones del Lenguaje y del Habla (TALP)
Universidad Politécnica de Cataluña

- URL: www.talp.upc.edu
- E-mail:
- Dirección: Campus Norte, Universidad Politécnica de Cataluña
- Rasgos: voz, multimodalidad biométrica

9.2. Otros organismos públicos españoles

Agencia Española de Protección de Datos (AEPD)

- URL: www.agpd.es
- Actividades: legislación y regulación

Asociación Española de Normalización y Certificación (AENOR)

- URL: www.aenor.es
- Actividades: normalización y certificación

Centro Criptológico Nacional (CCN)

- URL: http://www.ccn.cni.es/
- Actividades: autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica

Centro de Investigaciones Sociológicas (CIS)

- URL: www.cis.es
- Actividades: encuestas, estudios sociológicos

Centro Nacional de Inteligencia (CNI)

- URL: www.cni.es
- Actividades: investigación

Consejo Superior de Investigaciones Científicas (CSIC)

- URL: www.csic.es
- Actividades: investigación, becas, ayudas a la investigación y formación

esCERT - UPC

- URL: http://escert.upc.edu
- Actividades: ayuda y asesoramiento en seguridad informática y gestión de incidentes en redes telemáticas

Fábrica Nacional de Moneda y Timbre (FNMT)

- URL: www.fnmt.es
- Actividades: Entidad Pública de Certificación, certificación de firma electrónica, certificados de identidad de usuarios

Guardia Civil – Servicio de Criminalística de la Jefatura de Información y Policía Judicial

- URL: www.guardiacivil.es
- Actividades: informes periciales, identificación de personas, acústica forense, apoyo técnico-científico, miembro de la Red Europea de Institutos de Ciencias Forenses

Ministerio de Educación y Ciencia (MEC)

- URL: www.mec.es/ciencia/index.html
- Actividades: Planes Nacionales de I+D+i, becas, ayudas a la investigación y formación

Ministerio del Interior - Dirección General de Infraestructuras y Material de Seguridad de la Subsecretaría de Interior

- URL: www.mir.es/MIR/estrorganica/estructura/subsec/dgas1.html
- Actividades: planificación y coordinación de las políticas de infraestructuras y material en el ámbito de la seguridad

Ministerio del Interior - Secretaría de Estado de Seguridad

- URL: www.mir.es/SES
- Actividades: planes de infraestructura de la seguridad del Estado, elaboración de la inteligencia estratégica en la lucha contra todo tipo de delincuencia organizada, coordinación operativa

9.3. Ámbito internacional

Advanced Multimedia and Security Lab, Biometrics Group (AMSLBIO)
University of Magdeburg (Alemania)

- URL: http://wwwiti.cs.uni-magdeburg.de
- Rasgos: firma, escritura

Biometrics at GET: Bio-IDentity Lab
Groupe des Ecoles des Télécommunications (Paris, Francia)

- URL: http://www.int-evry.fr/biometrics
- Rasgos: firma, voz, cara, iris, multimodalidad biométrica

Biometric Consortium (BC)

- URL: http://www.biometrics.org
- Rasgos:

Biometric Research Center
San José State University (EE.UU.)

- URL: http://www.engr.sjsu.edu/biometrics
- Rasgos: cara, huella

Biometric Standards, Performance and Assurance Laboratory
Purdue University (EE.UU.)

- URL: http://www.biotown.purdue.edu
- Rasgos: iris, firma, huella, mano, cara, voz

Biometric Systems Laboratory (BioLab)
University of Bolonia (Italia)

- URL: http://biolab.csr.unibo.it
- Rasgos: huella, cara, mano, iris, firma, multimodalidad biométrica

Center for Biometrics and Security Research (CBSR)
Institute of Automation, Chinese Academy of Sciences -CASIA (China)

- URL: http://www.sinobiometrics.com
- Rasgos: cara, iris, huella, mano, escritura, modo de andar, multimodalidad biométrica

Center for Identification Technology Research (CITeR)
West Virginia University (EE.UU)

- URL: http://www.citer.wvu.edu
- Rasgos:

Centre for Vision, Speech and Signal Processing (CVSSP)
University of Surrey (Reino Unido)

- URL: http://www.ee.surrey.ac.uk/CVSSP
- Rasgos: cara, multimodalidad biométrica

Computer Laboratory
University of Cambridge (Reino Unido)

- URL: http://www.cl.cam.ac.uk/ jgd1000
- Rasgos: iris

Stichting Centrum voor Wiskunde en Informatica (CWI)
Amsterdam (Países Bajos)

- URL: http://www.cwi.nl
- Rasgos: cara, multimodalidad biométrica

Department of Architecture and Planning -Computer Vision Lab
University of Sassari (Italia)

- URL: www.architettura.uniss.it
- Rasgos: cara

Department of Electronics
University of Kent (Reino Unido)

- URL: http://www.ee.kent.ac.uk
- Rasgos: firma, escritura, huella, cara, multimodalidad biométrica

DoD's Biometric Management Office
Department of the Army (EE.UU.)

- URL: http://www.biometrics.dod.mil
- Rasgos:

European Biometric Forum (EBF)

- URL: http://www.eubiometricsforum.com
- Rasgos:

Informatics Department
University of Fribourg (Suiza)

- URL: http://www.unifr.ch/informatics
- Rasgos: voz, firma, cara, multimodalidad biométrica

Information: Signals, Images, Systems (ISIS)
University of Southampton (Reino Unido)

- URL: http://www.isis.ecs.soton.ac.uk
- Rasgos: modo de andar, oreja, cara

Institute of Digital Image Processing
Joanneum Research Graz (Austria)

- URL: http://www.joanneum.at/en/fb3/dib.html
- Rasgos: huella

Pattern Recognition and Image Processing Lab (PRIP)
Michigan State University (EE.UU)

- URL: http://biometrics.cse.msu.edu
- Rasgos: cara, huella, firma, mano, multimodalidad biométrica

School of Engineering Speech / Processing and Biometrics Group
Ecole Polytechnique Fédérale de Lausanne (Suiza)

- URL: http://www.epfl.ch
- Rasgos: voz, multimodalidad biométrica

Signal Analysis
Halmstad University (Suecia)

- URL: http://www2.hh.se/staff/josef/sa
- Rasgos: huella, cara, voz, multimodalidad biométrica

Signal and Image Processing Group (SIPG)
University of Bath (Reino Unido)

- URL: http://www.bath.ac.uk/elec-eng/research/sipg
- Rasgos: iris, cara

Signals and Systems Department (SaS)
University of Twente (Países Bajos)

- URL: http://www.sas.el.utwente.nl
- Rasgos: huella, cara

Speech and Image Processing Group
University of Wales Swansea

- URL: http://galilee.swan.ac.uk
- Rasgos: voz, cara

The Biometrics Resource Center
National Institute of Standards and Technology -NIST (EE.UU.)

- URL: http://www.itl.nist.gov/div893/biometrics
- Rasgos: huella, voz, cara

The Face Detection Home Page

- URL: http://www.facedetection.com
- Rasgos: cara

The Face Recognition Home Page

- URL: http://www.face-rec.org
- Rasgos: cara

The Iris Recognition Home Page

- URL: http://www.iris-recognition.org
- Rasgos: iris

Capítulo 10

El Séptimo Programa Marco de Investigación de la UE

10. El Séptimo Programa Marco de Investigación de la UE

10.1. Los Programas Marco de la UE

Los Programas Marco (PM) de la Unión Europea constituyen los principales instrumentos de financiación por medio de los cuales la Unión Europea apoya las actividades de investigación y desarrollo, abarcando prácticamente la totalidad de disciplinas científicas [28]. Los PM son propuestos por la Comisión Europea y adoptados por el Consejo y el Parlamento Europeo siguiendo un procedimiento de decisión conjunta.

Los PM vienen aplicándose desde 1984 y abarcan un período de cinco años, solapándose el último año de cada PM y el primero del siguiente. No obstante, el Séptimo PM [72], operativo desde el 1 de enero de 2007, se ha propuesto que dure 7 años. La cantidad prevista de participación financiera de la UE en el Séptimo Programa Marco es de 50.521 millones de euros para el período 2007-2013. Por lo que respecta a las acciones de investigación y formación en materia nuclear realizadas en virtud del tratado de EURATOM [77], se prevé un presupuesto de 2.751 millones de euros para 2007-2011.

El Séptimo PM está organizado en cuatro **programas** que se corresponden con cuatro componentes básicos de la investigación europea, ver Figura 17:

- **Cooperación**, prestando apoyo a toda la gama de actividades de investigación realizadas mediante la cooperación transnacional, desde los proyectos y redes en colaboración a la coordinación de los programas de investigación de cada país. Involucra a todos los agentes (investigadores, industria y PYMES) y supone el principal programa del Séptimo PM, con casi el 65 % del presupuesto.

- **Ideas**, aumentando el dinamismo, la creatividad y la excelencia de la investigación europea en las fronteras del conocimiento en todos los ámbitos científicos y tecnológicos.

- **Personas**, reforzando de modo cuantitativo y cualitativo los recursos humanos de la investigación y la tecnología de Europa por medio de las llamadas Acciones Marie Curie.

- **Capacidades**, respaldando las infraestructuras de investigación, la investigación en beneficio de las PYMES y el potencial de investigación de las regiones europeas, así como estimular el pleno despliegue del potencial de investigación de la Unión.

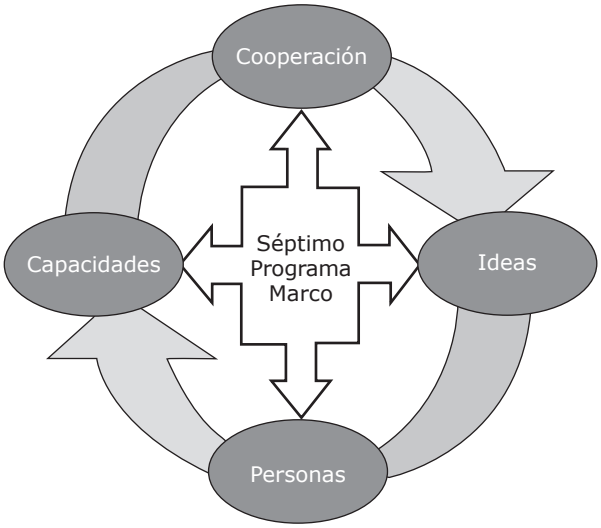


Figura 17. Estructura del Séptimo Programa Marco de la Unión Europea.

Dentro del programa de Cooperación, se definen una serie de **temas** que se corresponden con campos importantes en el progreso del conocimiento y la tecnología, donde la investigación se debe apoyar y reforzar para afrontar los retos sociales, económicos, ecológicos e industriales de Europa, teniendo en mente en todos ellos el objetivo general de contribuir al desarrollo sostenible.

Los diez temas que se han propuesto para la actuación comunitaria en el Séptimo PM son los siguientes:

- Salud
- Alimentación, agricultura y pesca, biotecnología
- Tecnologías de la información y la comunicación (TIC)
- Nanociencias, nanotecnologías, materiales y nuevas tecnologías de producción
- Energía
- Medio ambiente (incluido el cambio climático)
- Transporte (incluida la aeronáutica)

- Ciencias socioeconómicas y humanidades
- Espacio
- Seguridad

Junto a estos diez, hay dos temas más cubiertos por el Programa Marco de EURATOM:

- Investigación sobre la energía de fusión
- Fisión nuclear y radioprotección

10.2. Líneas del Séptimo Programa Marco relacionadas con el reconocimiento biométrico

Los dos temas principales que tienen relación con el reconocimiento biométrico son el de *seguridad* y el de *tecnologías de la información y la comunicación* (TIC). Entre los objetivos del tema de *seguridad* se encuentran desarrollar técnicas y conocimiento que contribuyan a la seguridad ciudadana, así como estimular la cooperación de todas las partes implicadas (usuarios e industria) con el fin de mejorar la competitividad y la efectividad en esta materia. La seguridad se define como un aspecto importante dentro de la política de la Unión Europea para asegurar la libertad y la justicia, a la vez que contribuye al desarrollo de otros temas de actuación como *transporte, energía, medio ambiente y salud*. Entre las actividades que se financiarían dentro del área de seguridad, encontramos:

- Seguridad ciudadana: soluciones tecnológicas para protección civil contra crimen y terrorismo.
- Seguridad de infraestructuras y servicios, tales como transporte, energía, servicios financieros y administraciones públicas.
- Vigilancia y control de fronteras.
- Seguridad en caso de crisis.
- Mejora de la integración, interconexión en interoperabilidad de sistemas de seguridad.
- Seguridad y sociedad, considerando la vertiente socio-económica, política, cultural, ética, etc. de la seguridad.

- Coordinación de investigación en seguridad entre distintos agentes nacionales e internacionales.

Por otro lado, el área de *tecnologías de la información y la comunicación* (TIC) supone el mayor punto de actuación del programa de Cooperación del Séptimo PM, ya que abarca el 28 % de presupuesto del programa de Cooperación y el 18 % de todo el Séptimo PM. Esta área se divide en siete "retos" de interés estratégico para la sociedad europea:

1. Aumento de las **infraestructuras de redes y servicios fiables**, abriendo la puerta a una variedad enorme de aplicaciones en red. Para ello, debe potenciarse el desarrollo y convergencia de todos los elementos implicados: equipamiento, dispositivos, redes de comunicaciones, software y e-servicios.

2. Desarrollo de sistemas y productos inteligentes y autónomos: **sistemas cognitivos y robótica**. Se trata de dotar a los sistemas automáticos de funcionalidades avanzadas de aprendizaje y razonamiento autónomo, siendo capaces de adaptarse a cambios en el entorno, así como a las preferencias y necesidades de cada usuario particular. Específicamente, se menciona como ejemplo el desarrollo de agentes automáticos de seguridad.

3. **Componentes, sistemas e ingeniería**, con el avance en el desarrollo de componentes electrónicos de nueva generación: dispositivos nanoelectrónicos, dispositivos fotónicos e integración de dispositivos electrónicos en todo tipo de productos de un modo eficiente y barato.

4. **Librerías digitales y contenidos**, siendo capaces de manejar el creciente flujo de información en la actual sociedad del conocimiento. La finalidad es hacer que el contenido y el conocimiento sean totalmente accesibles e interactivos tanto por las personas como por las máquinas.

5. **Cuidado de salud sostenible y personalizado**. Dado el actual envejecimiento de la población y el aumento de enfermedades crónicas, la demanda de servicios sociales y de salud no para de crecer. En este sentido, es necesario responder a las necesidades de atención del usuario, incluyendo el manejo de información médica de modo seguro. Específicamente, se menciona el desarrollo de sistemas portátiles de monitorización personalizada y de diagnóstico remoto.

6. **Movilidad, desarrollo sostenible y eficiencia energética**, mencionándose específicamente el acceso seguro a información a través de servicios móviles en tiempo real, y el acceso a datos e infraestructuras remotas para monitorización de riesgos ambientales.

7. **Vida independiente e inclusión**, enfocado sobre todo a la Tercera Edad. El aumento de población mayor de 65 años está teniendo enorme impacto socio-económico y hace necesario un nuevo paradigma de servicios sociales y sanitarios. La complejidad, la accesibilidad y la usabilidad son varias de las barreras a las que mucha gente, especialmente los mayores, se enfrentan a la hora de utilizar sistemas de información y comunicaciones. En este sentido, se pretende mejorar la accesibilidad y usabilidad de estos sistemas, prolongando la independencia y la participación activa de la población en la economía y en la sociedad.

10.3. Proyectos del Programa Marco relacionadas con el reconocimiento biométrico

A continuación se incluye una lista resumida de algunos proyectos de I+D+i relacionados con el reconocimiento biométrico que han sido financiados por Programas Marco de la UE:

- *PRIME-Privacy and Identity Management for Europe* (https://www.primeproject.eu) para el desarrollo de un sistema de gestión de la identidad controlado por el usuario.

- *GUIDE-Creating a European Identity Management Architecture for eGovernment* (http://istrg.som.surrey.ac.uk/projects/guide) para la creación de una arquitectura segura e interoperable que permita gestionar la identidad personal de los usuarios de servicios y transacciones electrónicas gubernamentales.

- *SERENITY-System Engineering for Security and Dependability* (http://www.serenity-project.org).

- *SecurePhone* (http://www.secure-phone.info) para el desarrollo de un sistema de comunicaciones sobre móviles 3G que haga uso de identificación biométrica.

- *FDIS-Future of Identity in the Information Society* (http://www.fidis.net), red de excelencia relacionada con tecnologías para identificación, con énfasis en temas de privacidad, seguridad, robo de identidad y implicaciones forenses.

- *BioHealth* (http://www.gsf.de/imei/biohealth), centrado en seguridad para servicios sanitarios electrónicos.

- *CyberSecurity* (http://cybersecurity.jrc.it), relacionado con la seguridad online.

- *Liberty Alliance Project* (http://www.projectliberty.org) orientado a posibilitar un mundo interconectado basado en estándares abiertos donde consumidores, ciudadanos, empresas e instituciones públicas puedan llevar a cabo transacciones online de modo seguro.

- *Pay By Touch* (http://www.paybytouch.com) cuyo objetivo es proporcionar mecanismos de autenticación biométrica para pagos.

- *BioSec IP*, orientado a solucionar problemas asociados con la resistencia a ataques, fiabilidad de los sistemas biométricos, privacidad, incompatibilidad de componentes, usabilidad, etc.

- *Biosecure NoE* (http://www.biosecure.info), red de excelencia que integra a los principales grupos investigadores de reconocimiento biométrico europeos.

Capítulo 11

El Plan Nacional de I+D+i

11. El Plan Nacional de I+D+i

Los Planes Nacionales [63] son el instrumento de programación de la I+D y la innovación tecnológica de la Administración General del Estado. Contemplado como Plan de Investigación Científica y Desarrollo Tecnológico en la Ley de la Ciencia (Ley 13/1986), y denominado desde el año 2000 Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica (I+D+i), es el mecanismo para establecer los objetivos y prioridades de la política de investigación e innovación a medio plazo, así como para diseñar los instrumentos que garanticen su consecución. Los Planes Nacionales tienen una duración de cuatro años. Actualmente está vigente el Plan 2004-2007 y se acaba de aprobar el Plan 2008-2011 [64].

11.1. El Plan 2004-2007

El Plan Nacional de I+D+i 2004-2007 (ver Figura 18) se aprobó en reunión del Consejo de Ministros el 7 de Noviembre de 2003, constituyendo el eje estratégico de la política española de I+D+i para su periodo de aplicación. Su elaboración contó con una amplia participación de todo el sistema de Ciencia- Tecnología-Empresa-Sociedad (más de 450 expertos de universidades, organismos públicos, centros tecnológicos y empresas), incluidas las Comunidades Autónomas, departamentos ministeriales y otras instancias (Consejo Asesor, Consejo Económico y Social).

El Plan define una serie de **objetivos estratégicos** sobre los que se vertebrarán las diferentes **actuaciones**: incremento del nivel de la ciencia y la tecnología españolas; aumento de los recursos humanos dedicados a la I+D+i, tanto en el sector público, como en el privado; refuerzo de los derechos y las garantías de los investigadores; fortalecimiento de la dimensión internacional de la ciencia y la tecnología españolas, especialmente en el Espacio Europeo de Investigación; nuevas actuaciones en grandes instalaciones; potenciación del papel de la investigación básica, y mejora de la comunicación a la sociedad de los avances que se vayan produciendo.

Dentro de este Plan, se fijan varias **actuaciones**. En primer lugar, establece acuerdos sectoriales con los diferentes segmentos productivos. Además, y para motivar la necesaria inversión en I+D, prevé mejoras fiscales a la inversión en Investigación y Desarrollo, a través de mayores deducciones directas; el incremento de la deducción para gastos de personal investigador; el incremento de la base de deducción para la adquisición de patentes, licencias y diseños, así como la elevación del límite aplicable a la deducción por I+D+i en las tecnologías de información y la comunicación.

Junto al marco fiscal, el Plan estipula el apoyo a la creación de nuevas empresas de base tecnológica a través de Incubadoras y Capital riesgo, así como una mayor coordinación en la interacción público-privado, a través del soporte a parques científicotecnológicos; apoyo a las Oficinas de Transferencia de Resultados de Investigación (OTRIS) y apoyo a los Centros Tecnológicos o la creación de Plataformas Tecnológicas. También tendrá una especial dedicación el apoyo financiero a la creación de unidades de I+D y a la protección intelectual e industrial.

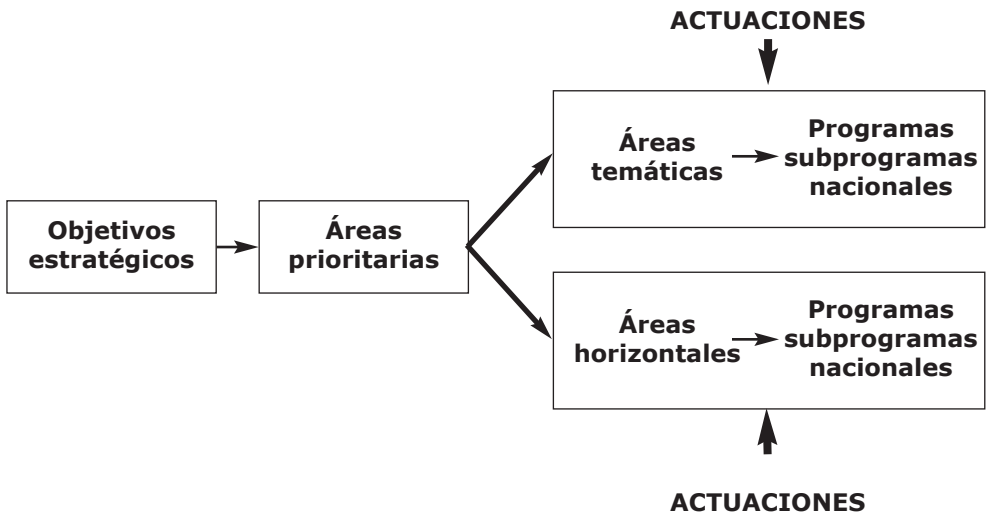


Figura 18. Estructura del Plan Nacional de I+D+i 2004-2007.

Se define como **área prioritaria** del Plan Nacional a un conjunto de temas interrelacionados, agrupados en torno a **programas nacionales**, en los que se plantean determinados objetivos científico-tecnológicos relacionados con los objetivos estratégicos del Plan Nacional. Algunos de estos temas se agrupan en **subprogramas**. Adicionalmente, cada uno de los programas nacionales comprende también un conjunto de temas no sometidos a prioridades, fundamentalmente ligados a la investigación básica no orientada. Se distinguen dos tipos de **áreas prioritarias**: áreas temáticas, en las que el dominio científico-tecnológico de actuación está claramente definido, y **áreas horizontales**, abiertas a todos los dominios científico-tecnológicos.

En el Plan Nacional 2004-2007 se definen las siguientes **áreas temáticas**, dentro de las cuales se engloban un total de 25 programas nacionales:

- Área de ciencias de la vida
- Área de ciencias y tecnologías agroalimentarias y medioambientales
- Área de ciencias del espacio, matemáticas y físicas
- Área de energía
- Área de química, materiales y diseño y producción industrial
- Área de seguridad y defensa
- Área de tecnologías de la sociedad de la información
- Área de transporte y construcción
- Área de humanidades, ciencias sociales y económicas

Asimismo, las **áreas horizontales** definidas en el Plan Nacional 2004-2007 son:

- Área de cooperación internacional
- Área de recursos humanos
- Área de competitividad empresarial
- Área de equipamiento en infraestructura
- Área de cultura científica y tecnológica

11.2. El reconocimiento biométrico en el Plan 2004-2007

Dentro del área temática de seguridad y defensa, el *programa nacional de seguridad* hace referencia explícita al reconocimiento biométrico. Las prioridades temáticas de dicho programa que le conciernen son:

- **Identificación de personas y objetos**, mencionando como línea de actuación específica el desarrollo de sistemas de identificación biométrica de personas.

- **Vigilancia y seguimiento de personas o bienes**, teniendo como líneas de actuación el desarrollo de sistemas avanzados de vigilancia personal para facilitar el seguimiento electrónico de personas, así como la detección de intrusos.

- **Protección de información**, teniendo entre sus líneas de actuación la seguridad en las comunicaciones y la identificación segura de información.

- **Sistemas de investigación forense**, mencionando específicamente el desarrollo de técnicas de investigación de huellas.

Asimismo, el reconocimiento biométrico tiene cabida en el área temática de *tecnologías de la sociedad de la información*. Por un lado, algunas de las prioridades temáticas del *programa nacional de tecnologías informáticas* son:

- **Sistemas inteligentes**, permitiendo dotar de autonomía y capacidad de comunicación a las nuevas demandas creadas por el desarrollo de Internet y los nuevos modelos de comunicación entre usuarios, empresas y administraciones.

- **Gestión de información**, permitiendo gestionar de forma eficiente crecientes volúmenes de contenido y hacerlos accesibles a sus destinatarios.

- **Interfaces avanzados**, permitiendo integrar reconocimiento de habla, escritura, expresión humana, gestos, etc.

- **Sistemas distribuidos y abiertos**, con el desarrollo de servicios electrónicos como respuesta a las necesidades de la sociedad de la información.

- **Infraestructuras complejas inteligentes**, desarrollando tecnologías aplicadas a infraestructuras de transporte, energía, producción agraria o industrial, para mejorar su capacidad, eficiencia y seguridad.

Por otro lado, también dentro del área temática de *tecnologías de la sociedad de la información*, entre las prioridades del *programa nacional de tecnologías de servicios de la sociedad de la información* encontramos:

- **e-negocio**, desarrollando las herramientas y procedimientos informáticos necesarios para la plena integración del concepto de e-negocio.

- **e-pyme**, consiguiendo que las PYMES informaticen sus procesos internos de negocio mediante la incorporación de aplicaciones que les permitan interactuar e integrar sus relaciones con otros agentes.

- **e-formación**, flexibilizando las restricciones espacio-temporales que conlleva la formación presencial.

- **e-administración**, mejorando la calidad del servicio público, evitando desplazamientos y mejorando los tiempos de respuesta.

- **e-hogar**, promoviendo nuevos servicios hacia el hogar en los ámbitos de educación, sanidad, entretenimiento, administración, etc.

- **e-inclusión**, creando soluciones dirigidas a colectivos desfavorecidos.

- **e-asistencia**, trasladando ciertos servicios asistenciales al hogar.

11.3. El Plan 2008-2011

El nuevo Plan Nacional de I+D+i 2008-2011 (ver Figura 19) se aprobó en reunión del Consejo de Ministros el 14 de Septiembre de 2007. Los numerosos diagnósticos realizados sobre el Sistema Español de Ciencia y Tecnología (SECYT) en los años de vigencia del Plan 2004-2007 han apuntado la necesidad de que el nuevo Plan Nacional de I+D+i 2008-2011 incorpore cambios importantes en su estructura y en su forma de gestión. Se trata, ahora, de superar un modelo de Plan Nacional que está basado en áreas temáticas para pasar a un modelo de Plan construido a partir de la definición de los instrumentos, donde éstos son la respuesta de las Administraciones Públicas a los objetivos estratégicos y operativos fijados en la Estrategia Nacional de Ciencia y Tecnología (ENCYT).

Los **objetivos estratégicos** del Plan Nacional de I+D+i 2008-2011 se han identificado teniendo en cuenta los principios básicos y objetivos recogidos en la ENCYT, y son los que han marcado el diseño de los instrumentos y los programas nacionales del mismo. Son objetivos estratégicos de la ENCYT: situar a España en la vanguardia del conocimiento; promover un tejido empresarial altamente competitivo; desarrollar una política integral de ciencia, tecnología e innovación; la imbricación de los ámbitos regionales en el sistema de ciencia y tecnología; avanzar en la dimensión internacional como base para el salto cualitativo del sistema; conseguir un entorno favorable a la inversión en I+D+i; y fomentar la cultura científica y tecnológica de la sociedad.

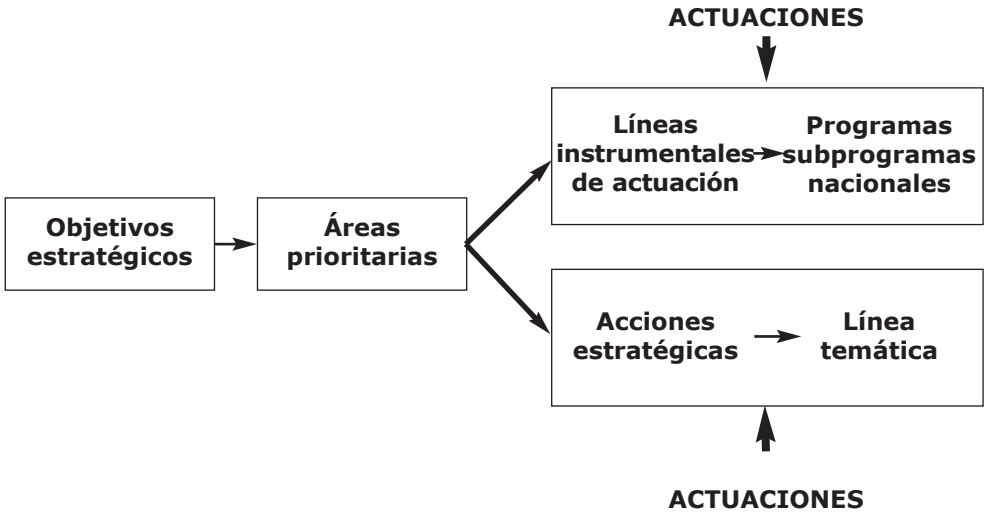


Figura 19. Estructura del Plan Nacional de I+D+i 2008-2011.

Las **áreas de actuación** fijadas dentro del Plan 2008-2011 para la consecución de sus objetivos estratégicos incluyen:

- **Generación de Conocimientos y de Capacidades Científicas y Tecnológicas**, relacionada con la financiación de la investigación de carácter básico o fundamental, con la capacitación de recursos humanos y la disponibilidad del equipamiento e infraestructuras.

- **Fomento de la Cooperación en I+D**, dirigida a fomentar la cooperación entre agentes y con el marco internacional y regional como escenario básico.

- **Desarrollo e Innovación Tecnológica Sectorial**, orientado a reducir el déficit investigador de las empresas españolas, incentivando el desarrollo en las mismas de conocimiento propio y fomentando la cultura científica y tecnológica de la sociedad, aprovechando los nuevos formatos de comunicación, desarrollando estructuras estables generadoras y promotoras de cultura científica e instalando nodos en red de comunicación científica y tecnológica.

- **Acciones Estratégicas**, con un concepto integral en el que se pongan en valor las investigaciones realizadas, así como su transformación en procesos, productos y servicios para la sociedad.

Al igual que en el Plan 2004-2007, se definen unas **áreas prioritarias**: las **Líneas Instrumentales de Actuación (LIA)**, equivalentes a las áreas temáticas, y las **Acciones Estratégicas**, equivalentes a las áreas horizontales. Las primeras ahora no se definen de acuerdo a un dominio científico tecnológico concreto, sino que agrupan un conjunto de instrumentos que tienen la misión de responder a los objetivos estratégicos formulados en la ENCYT y, por ende, a los objetivos planteados en el propio Plan Nacional. Por otro lado, las segundas Acciones Estratégicas siguen correspondiendo a sectores o tecnologías de carácter horizontal.

En el Plan Nacional 2008-2011 se definen las siguientes **Líneas Instrumentales de Actuación**, en las cuales se engloban un total de 13 Programas Nacionales:

- Línea instrumental de Recursos Humanos
- Línea instrumental de Proyectos de I+D+i
- Línea instrumental de fortalecimiento institucional
- Línea instrumental de infraestructuras científicas y tecnológicas
- Línea instrumental de utilización del conocimiento y transferencia tecnológica
- Línea instrumental de articulación e internacionalización del sistema

Igualmente, las **Acciones Estratégicas** definidas en el Plan Nacional 2008- 2011, las cuales engloban un total de 23 líneas temáticas, son:

- Acción estratégica de Salud
- Acción estratégica de Biotecnología
- Acción estratégica de Energía y Cambio Climático
- Acción estratégica de Telecomunicaciones y Sociedad de la Información
- Acción estratégica de Nanociencia y Nanotecnología, Nuevos Materiales y Nuevos Procesos Industriales

Aunque el Plan Nacional 2008-2011 posee una estructura que se mantendrá inalterable a lo largo de sus cuatro años de vigencia, sus Programas

Nacionales y convocatorias serán objeto de actualización anual con motivo de nuevas necesidades o demandas de los actores del sistema. Así, dentro de cada Programa Nacional podrán replantearse anualmente las prioridades, las actividades a emprender, la asignación de recursos a las mismas y las posibles nuevas acciones estratégicas, pudiendo incluso suscitarse el interés de algún nuevo programa, o detectarse la falta de pertinencia de alguno de los existentes. De este modo, anualmente se elaborará el Programa de Trabajo del Plan Nacional que actuará como herramienta de actualización dinámica y programación a corto plazo. El Programa de Trabajo anual incluye, principalmente, el calendario previsto de convocatorias públicas, con indicación de los plazos de presentación y de resolución de propuestas, la distribución económica del presupuesto anual por áreas y programas prioritarios y los organismos de gestión de cada una de las actuaciones. Con fecha 17 de Septiembre de 2007 se aprobó el Programa de Trabajo 2008, el cual prevé comprometer unos fondos totales de 8.078,48 millones de euros distribuidos como sigue:

- Líneas Instrumentales de Actuación (LIAs): 4.369,16 millones de euros para convocatorias públicas y de concurrencia competitiva, distribuidos de acuerdo a la Figura 20.

- Acciones Estratégicas: 1.282,46 millones de euros para convocatorias públicas y de concurrencia competitiva, distribuidos de acuerdo a la Figura 21.

- Otras actuaciones de fomento de la I+D+I que no se financian a través de convocatorias públicas y de concurrencia competitiva: 2.415,49 millones de euros, distribuidos por LIA de acuerdo a la Figura 22.

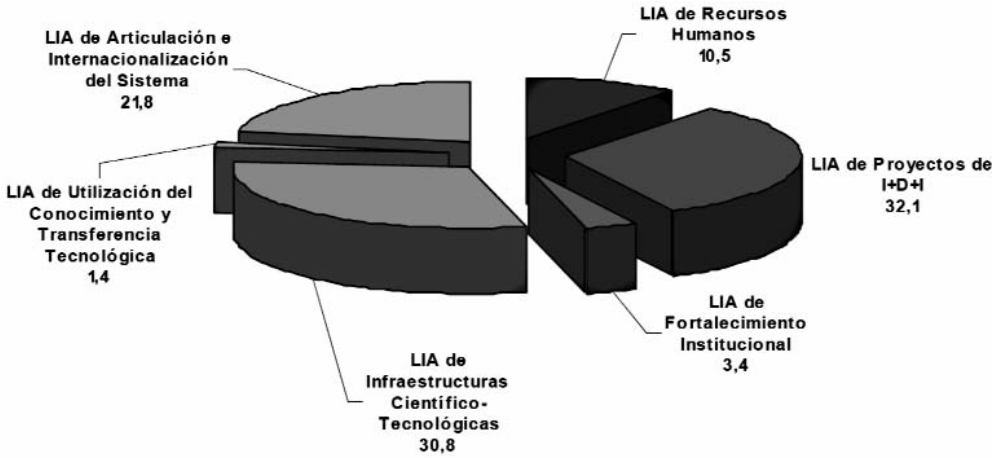


Figura 20. Distribución presupuestaria (en %) prevista para el año 2008 por Línea Instrumental de Actuación del Plan Nacional de I+D+i 2008-2011 (convocatorias públicas y de concurrencia competitiva).

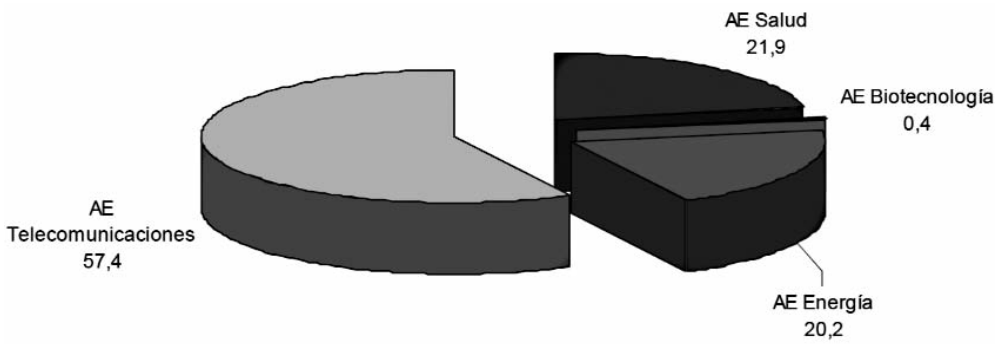


Figura 21. Distribución presupuestaria (en %) prevista para el año 2008 por Acción Estratégica del Plan Nacional de I+D+i 2008-2011 (convocatorias públicas y de concurrencia competitiva).

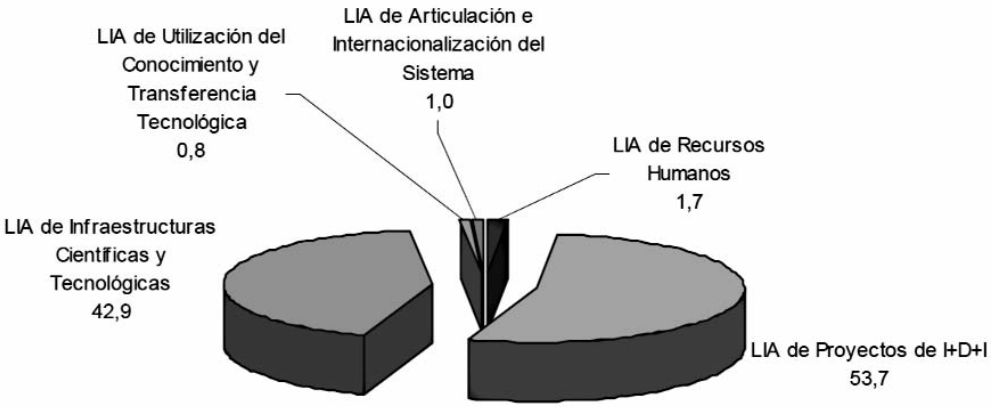


Figura 22. Distribución presupuestaria (en %) prevista para el año 2008 por Línea Instrumental de Actuación del Plan Nacional de I+D+i 2008-2011 (acciones no financiables a través de convocatorias públicas y de concurrencia competitiva).

11.4. El reconocimiento biométrico en el Plan 2008-2011

Entre las líneas instrumentales del Plan 2008-2011, el reconocimiento biométrico tiene cabida en la *línea instrumental de Proyectos de I+D+i*. Dicha línea comprende programas nacionales de proyectos de investigación fundamental, aplicada, desarrollo experimental e innovación. Sus objetivos son favorecer la generación de nuevo conocimiento, la aplicación del conocimiento existente a la solución de problemas, así como la explotación del mismo para la innovación y generación de nuevos productos, procesos o servicios o para obtener una mejora sustancial en los ya existentes.

Por otro lado, tenemos la *acción estratégica de Telecomunicaciones* y *Sociedad de la Información*, cuyo objetivo fundamental es conseguir el adecuado desarrollo y utilización de las tecnologías, aplicaciones, servicios y contenidos de la Sociedad de la Información para contribuir al éxito de un modelo de crecimiento económico basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional, la accesibilidad universal y la mejora del bienestar y la calidad de vida de los ciudadanos. Los objetivos concretos de esta acción estratégica que se indican en el Plan 2008-2011 que caen dentro del ámbito de actuación del reconocimiento biométrico son: promover un tejido empresarial altamente competitivo, promover servicios públicos digitales y de calidad,

facilitar la educación en la era digital y desarrollar un nuevo contexto digital basado, entre otros, en la e-confianza para los servicios de la Sociedad de la Información. Entre las tecnologías implicadas que se mencionan explícitamente en el Plan 2008-2011 para la consecución de estos objetivos, el reconocimiento biométrico tiene relación con las siguientes: interfaces multimodales avanzados, tecnologías de procesamiento del lenguaje humano, sistemas inteligentes, identificación y control, seguridad de infraestructuras, protección y seguridad de datos, propiedad intelectual y fraudes, seguridad en entornos físicos, Administración Electrónica, programas de inclusión para personas con necesidades especificas, comercio electrónico, salud, asistencia social y seguridad en general.

Capítulo 12

Planes Regionales de I+D+i

12. Planes Regionales de I+D+i

De la misma manera que la Administración General del Estado promueve el Plan Nacional de I+D+i, cada una de las Administraciones Autonómicas posee su propio plan. En esta sección se describen brevemente o se referencian los de cada Comunidad Autónoma.

12.1. Comunidad de Madrid: IV PRICIT 2005-2008

En Abril de 2005, el Consejo de Gobierno de la Comunidad de Madrid aprobó el IV Plan Regional de Investigación Científica e Innovación Tecnológica (IV PRICIT) para el periodo 2005-2008 [42]. En su elaboración tomaron parte 34 instituciones y 290 expertos, junto con la canalización a través de Internet de la participación ciudadana, con más de 700.000 visitas a la página donde se expusieron los documentos en elaboración. Igualmente, se ha tenido en cuenta el contexto nacional y europeo donde se enmarca, con atención al Espacio Europeo de Enseñanza Superior, al contenido del Sexto Programa Marco 2002-2006 de la Unión Europea y al V Programa Nacional de I+D+i 2004- 2007.

El IV PRICIT, dotado con un presupuesto total de actuación de 225 millones de euros para el periodo 2005-2008 atenderá las principales demandas del sistema regional de ciencia y tecnología: creación de capital humano para la I+D estableciendo una carrera publica de investigador, mejora de la competitividad de los investigadores de la Comunidad de Madrid y su relación con las demandas sociales y productivas, coordinación de las infraestructuras de I+D+i de interés regional, fomento de la cooperación y de la I+D+i empresarial, desarrollo de un marco de cooperación interregional con otras comunidades autónomas y promoción de los valores de la cultura científico tecnológica. La misión genérica del IV PRICIT puede formularse en los siguientes términos: hacer de Madrid un nodo de creciente importancia dentro de la red europea y global de "regiones del conocimiento", impulsando su desarrollo, y considerando a la ciencia y a la tecnología como elementos básicos en la creación de riqueza, de bienestar social y de creatividad cultural.

El IV PRICIT considera 10 áreas científico-tecnológicas estratégicas, las cuales a su vez abarcan un total de 97 líneas específicas de trabajo:

- Bienes de equipo, diseño y producción industrial.
- Energía.
- Materiales y nanotecnología.

- Tecnologías agroalimentarias.
- Tecnologías de la información y de las comunicaciones.
- Ciencias de la salud y biotecnología.
- Recursos naturales y tecnologías medioambientales.
- Productos y procesos químicos.
- Socioeconomía, humanidades y derecho.
- Ciencias del espacio, físicas y matemáticas.

Aparte de las áreas anteriores, el IV PRICIT también considera 3 líneas de investigación de interés especial:

- Áreas básicas de conocimiento Biomédicas.
- Tecnología de sensores.
- Genómica, Transcriptómica, Proteómica y Metabolómica.

12.2. Comunidad de Cataluña: PRI 2005-2008

El Plan de Investigación e Innovación (PRI) de Cataluña 2005-2008 [60] fue aprobado por el pleno del Consejo Interdepartamental de Investigación e Innovación Tecnológica (CIRIT) el día 28 de Diciembre de 2004 y por el Consejo Ejecutivo de la Generalitat de Catalunya el 25 de Enero de 2005.

La misión del PRI 2005-2008 es situar a Cataluña en una posición avanzada en Europa por lo que respecta al sistema de investigación e innovación mediante una política pública coordinada con el conjunto de agentes públicos y privados que promueva la sociedad del conocimiento y la iniciativa emprendedora con el fin de conseguir un desarrollo económico sostenible que aporte bienestar y cohesión social. Para cumplir con sus objetivos el Plan de Investigación e Innovación 2005-2008 se estructura en *actuaciones transversales* y *actuaciones complementarias*. Asimismo se han establecido *líneas prioritarias de investigación* y se ha definido una *estrategia sectorial y tecnológica*.

Las *actuaciones transversales* comprenden todas las acciones destinadas a reforzar la cadena de valor del conocimiento y la tecnología en todos los

sectores de la economía: la consecución de la masa crítica y la perfección de los sistemas de generación del conocimiento en todos los ámbitos, la optimización de los mecanismos de transferencia del conocimiento científico y tecnológico que pueda ser utilizado por el tejido empresarial, la creación de un sistema productivo exigente y con capacidad de absorción, y la dotación de herramientas financieras para minimizar los riesgos que pudiera generar esta absorción de tecnología nueva. Las *actuaciones complementarias* por su parte tienen como finalidad generar un entorno que potencie la cultura de la ciencia, la tecnología y la innovación en todos los ámbitos de la sociedad, así como el surgimiento y la proyección de iniciativas innovadoras. Para ello se incluyen programas de movilidad y cooperación, fomento y comunicación de la cultura científica y tecnológica, fomento de la iniciativa emprendedora y coordinación y atracción de recursos estatales y europeos.

En cuanto a las *líneas prioritarias de investigación*, el PRI 2005-2008 prioriza las siguientes líneas de interés estratégico para los sectores productivos:

- Investigación biomédica y en ciencias de la salud
- Investigación en ingenierías de tecnologías de la información y la comunicación (TIC)
- Investigación en ciencia y tecnología agroalimentaria
- Investigación en desarrollo social y cultural
- Investigación en sostenibilidad y medio ambiente

Además, se potencian dentro del PRI 2005-2008 las líneas de gran transversalidad como la investigación en nanociencia y nanotecnología. Por otro lado, aparte del fomento de estas líneas, se contempla una *estrategia sectorial y tecnológica*. Dentro de esta estrategia, se incide específicamente en un conjunto de sectores estratégicos de alto potencial de crecimiento y de elevado contenido tecnológico, con acciones diferenciadas en función del sector, y en un conjunto de tecnológicas específicas capaces de generar ventajas competitivas diferenciales en estos sectores estratégicos, y que se extiendan al resto del tejido empresarial a través de las diferentes infraestructuras de apoyo a la transferencia de tecnología. Dichos sectores son: aeroespacial, biotecnología, industria farmacéutica, sector de la alimentación de segunda generación y la industria vinculada a las energías renovables. Por otro lado, las tecnologías específicas son: tecnologías de la producción, nuevos materiales, nanotecnología, tecnologías de la

información y las comunicaciones (TIC), tecnologías energéticas, biotecnología y ciencias de la organización.

12.3. Otros planes o instituciones regionales de investigación

- Castilla La Mancha Innovación [15]
- Departamento de Educación, Universidades e Investigación. Gobierno Vasco [22].
- Estrategia Regional de Investigación Científica, Desarrollo Tecnológico e Innovación de Castilla y León 2007-2013 [27].
- Fundación para el Fomento en Asturias de la Investigación Científica Aplicada y la Tecnología (FICYT) [33].
- Instituto Tecnológico de Aragón [40].
- Plan Andaluz de Investigación [7].
- Plan de Ciencia, Tecnología e Innovación de las Illes Balears 2005-2008 [59].
- Plan Estratégico de Innovación, Ciencia y Tecnología (In.Ci.Te) de Galicia 2006-2010 [61].
- Plan Integrado Canario I+D+i [62].
- Plan Regional I+D+i de Cantabria (PRIDI) [65].
- Plan Riojano de I+D+i 2003-2007 [66].
- Plan Tecnológico de Navarra [67].
- Plan Valenciano de Investigación Científica, Desarrollo Tecnológico e Innovación [68].

Referencias

Referencias

1. Agència Catalana de Protecció de Dades (APDCAT), http://www.apdcat.net/

2. Agencia Española de Protección de Datos (AEPD). www.agpd.es.

3. Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), http://www.madrid.org/apdcm

4. Agencia Vasca de Protección de Datos, http://www.avpd.euskadi.net/s04-5213/es/

5. F. Alonso-Fernández, Julián Fierrez, Javier Ortega-García, Joaquín González-Rodríguez, H. Fronthaler, K. Kollreider, and J. Bigun. "A comparative study of fingerprint image quality estimation methods". *IEEE Trans. on Information Forensics and Security*, Vol. 2, Num. 4, pp. 734- 743, December 2007.

6. American National Standards Institute (ANSI). www.ansi.org.

7. Andalucía Investiga. www.andaluciainvestiga.com.

8. Artículo 29 - Grupo de Protección de Datos, "Working Document on Biometrics", European Commission Justice and Home Affairs, Policy papers 12168/02/ES WP 80, 1 de Agosto de 2003, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_es.pdf

9. Asociación Española de Normalización y Regulación (AENOR). www.aenor.es.

10. BC. Biometrics Consortium, www.biometrics.org, 2005.

11. BioAPI. BioAPI consortium, Biometric Application Programming Interface, www.bioapi.org. 1998.

12. BITE, Biometric Identification Technology Ethics, http://www.biteproject.org/

13. BMEC. The BioSecure Multimodal Evaluation Campaign http://www.intevry.fr/biometrics/BMEC2007/index.php, 2007.

14. R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior, editors. "Guide to Biometrics". Springer Verlag, 2004.

15. Castilla La Mancha Innovación. www.clminnovacion.com.

16. CBEFF. Common Biometric Exchange File Format, 2001 http://www.itl.nist.gov/ div893/ biometrics/ documents/ NIS IR6529A.pdf

17. Centro Criptológico Nacional (CCN). www.ccn.cni.es.

18. Comité Consultatif National d'Ethique (CCNE), http://www.comiteethique. fr/

19. Commission Nationale de l'Informatique et des Libertés (CNIL), http://www.cnil.fr/

20. Council of Europe, Legal Affaires, "Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data", 2005, ttp://www.coe.int/t/e/legal_affairs/legal_cooperation/ data_protection/documents/reports_and_studies_of_data_protecti on_committees/O-Biometrics(2005)_en.asp

21. Data Protection, European Commission Justice and Home Affairs, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

22. Departamento de Educación, Universidades e Investigación. Gobierno Vasco. www.hezkuntza.ejgv.euskadi.net.

23. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, http://eur-lex.europa.eu/ LexUriServ/ exUriServ.do?uri= CELEX: 31995L0046: ES: HTML

24. DoD. Biometrics Management Office, Department of Defense www.biometrics.dod.mil, 2007.

25. A. Drygajlo, Speech Processing an Biometrics Group, Signal rocessing Institute, Ecole Polytechnique Fédérale de Lausanne (EPFL), Biometric Lecture 13, 2007- 8, http://scgwww.epfl.ch/courses/Biometrics-Lectures- 2007-2008-pdf/13-Biometrics-Lecture-13-2007-12-17.pdf

26. EBF. European Biometrics Forum, www.eurobiometricforum.com, 2003.

27. Estrategia Regional de Investigación Científica, Desarrollo Tecnológico e Innovación de Castilla y León 2007-2013. www.jcyl.es.

28. European Research Portal. www.ec.europa.eu/research.

29. European Treaty Series–No. 108, "Convention for the Protection of Individuals with Regard to Automatic Processing Personal Data", Strasbourg, 28.01.1981, http://conventions.coe.int/ Treaty/ en/ Treaties/ Html/ 108.htm.

30. FIDIS, Future of Identity in the Information Society, http://www.fidis.net/

31. J. Fierrez and J. Ortega-García. "Handbook of Biometrics", chapter "Online signature verification". Springer, 2007.

32. FRVT. Face Recognition Vendor Test, http://www.frvt.org. 2006.

33. Fundación para el Fomento en Asturias de la Investigación Científica Aplicada y la Tecnología (FICYT). www.ficyt.es.

34. FVC2006. Fingerprint Verification Competition http://bias.csr.unibo.it/fvc2006/default.asp. 2006.

35. J. Galbally, J. Fierrez, and J. Ortega-García. "Vulnerabilities in biometric systems: attacks and recent advances in liveness detection". *Proc. Spanish Workshop on Biometrics, SWB*, Girona, Spain, 2007.

36. IBG. International Biometric Group, www.biometricgroup.com, 2007.

37. ICE. Iris Challenge Evaluation, http://iris.nist.gov/ice. 2006.

38. INCITS M1. InterNational Committee for Information Technology Standards, Technical Committee M1, Biometrics (INCITS M1) http://m1.incits.org, 2007.

39. Instituto Nacional de Tecnologías de la Comunicación (INTECO). www.inteco.es.

40. Instituto Tecnológico de Aragón. www.ita.es.

41. ISO/IEC JTC1 SC37. ISO/IEC JTC1 on Information technology, SC37 on Biometrics, www.jtc1.org/sc37, 2002.

42. IV Plan Regional de Investigación Científica e Innovación Tecnológica de la Comunidad de Madrid (IV PRICIT). www.madrimasd.org/queesmadrimasd/pricit/default.asp.

43. A.K. Jain and A. Ross. "Multibiometric systems". *Communications of the ACM, Special Issue on Multimodal Interfaces*, 47(1):34–40, January 2004.

44. A.K. Jain, A. Ross, and S. Pankanti. "Biometrics: A tool for information security". *IEEE Transactions on Information Forensics and Security*, 1:125–143, 2006.

45. A.K. Jain, A. Ross, and S. Prabhakar. "An introduction to biometric recognition". *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, January 2004.

46. Steven Levy. "Cripto. Cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital". Alianza Editorial. 2002.

47. LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Jefatura del Estado, BOE nº 298, 14 de Diciembre de 1999, http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

48. LEY ORGÁNICA 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Jefatura del Estado, BOE nº 262, 31 de octubre de 1992, http://www.boe.es/ boe/ dias/ 1992/ 10/ 31/ pdfs/A37037-37045.pdf

49. S. Z. Li and A. K. Jain, editors. "Handbook of Face Recognition". Springer Verlag, 2004.

50. D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. "Handbook of Fingerprint Recognition". Springer, New York, 2003.

51. A.J. Mansfield and J.L. Wayman. "Best Practices in Testing and Reporting Performance of Biometric Devices", v 2.01, 2002 http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf.

52. T. Mansfield, G. Kelly, D. Chandler, and J. Kane. "Biometric product testing final report". National Physical Laboratory, UK, 2001 www.cesg.gov.uk/site/ast/biometrics/media/BiometricsTestReportpt1.pdf

53. S. Nanavati, M. Thieme, and R. Nanavati, editors. "Biometrics: Identity Verification in a Networked World". Wiley, 2002.

54. National Institute of Standards and Technology (NIST). www.nist.gov.

55. NIST-ITL. The Biometrics Resource Center, Information Technology Laboratory, National Institute of Standards and Technology www.itl.nist.gov/div893/biometrics.

56. NIST SRE. NIST Speaker Recognition Evaluation http://www.nist.gov/speech/tests/spk/index.htm. 2006.

57. Opinion nº 98 del Comité Consultatif National d'Ethique (CCNE), "Biometrics, identifying data and human rights", 20 Junio de 2007, http://www.comite-ethique.fr/docs/en/avis098.pdf

58. J. Ortega-García, J. Bigun, D. Reynolds, and J. González-Rodríguez. "Authentication gets personal with biometrics". *IEEE Signal Processing Magazine*, 21:50– 62, 2004.

59. Plan de Ciencia, Tecnología e Innovación de las Illes Balears 2005-2008. www.caib.es.

60. Plan de Investigación e Innovación de Cataluña 2005-2008 (PRI). www10.gencat.net/pricatalunya/cas/index.htm.

61. Plan Galego de Investigación, Desenvolvemento e Innovación Tecnolóxica 20062010 (In.Ci.Te). www.dxid.org/.

62. Plan Integrado Canario I+D+i. www.gobiernodecanarias.org/educacion/.

63. Plan Nacional de I+D+i. www.mec.es/ciencia/plan idi.

64. Plan Nacional I+D+i 2008-2011. http://www.plannacionalidi.es/.

65. Plan Regional I+D+i de Cantabria (PRIDI). www.idican.es.

66. Plan Riojano de I+D+i 2003-2007. www.larioja.org/i+d+i/.

67. Plan Tecnológico de Navarra. www.plantecnologico.com.

68. Plan Valenciano de Investigación Científica, Desarrollo Tecnológico e Innovación. www.gva.es.

69. I. van der Ploeg, "Biometric Identification Technologies: Ethical Implications of the Informatization of the Body", BITE Policy Paper no. 1, Marzo 2005.

70. REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Ministerio de Justicia, BOE nº 151, 25 de Junio de 1999.
http://www.boe.es/boe/dias/1999/06/25/pdfs/A24241- 24245.pdf

71. REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Ministerio de Justicia, BOE nº 17, 19 de Enero de 2008, http://www.boe.es/ boe/ dias/ 2008/01/19/pdfs/A04103-04136.pdf

72. Seventh Research Framework Programme (FP7).
www.ec.europa.eu/research/fp7.

73. K. Strandburg, D. Stan Raicu (Editors), "Privacy and Technologies of Identity: A Cross-Disciplinary Conversation", Springer, 2006.

74. SVC. Signature Verification Competition,
http://www.cs.ust.hk/svc2004. 2004.

75. M. Tapiador and J.A. Sigüenza, editores. Tecnologías Biométricas aplicadas a la Seguridad. RA-MA Editorial, 2005.

76. The Biometric Consortium. Biometric system vendors.
www.biometrics.org/biomvendors.htm.

77. Treaty establishing the European Atomic Energy Community (Euratom). http://europa.eu.

78. J. Wayman, A. Jain, D. Maltoni, and D. Maio, editors. "Biometric Systems: Technology, Design and Performance Evaluation". Springer, 2005.