POLITÉCNICA
"Ingeniamos el futuro"

CAMPUS
DE EXCELENCIA
INTERNACIONAL

Biometría

Capacidades de I+D, soluciones tecnológicas y empresas UPM

Universidad Politécnica de Madrid

Informe realizado por el Área de Innovación, Comercialización y Creación de Empresas
Vicerrectorado de Investigación – Universidad Politécnica de Madrid

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

Informe realizado por el Área de Innovación, Comercialización y Creación de Empresas – Vicerrectorado de Investigación – Universidad Politécnica de Madrid.

Universidad Politécnica de Madrid:
Área de Innovación, Comercialización y Creación de Empresas
Vicerrectorado de Investigación
Universidad Politécnica de Madrid
e: innovacion.tecnologica@upm.es
w: http://www.upm.es

Índice

1. Introducción

El desarrollo tecnológico biométrico, en términos generales, se encuentra ya en un estado maduro, y el interés por implementar sistemas biométricos globales para la seguridad es creciente, impulsado por ejemplo por la amenaza global terrorista de los últimos años y la necesidad de regular el paso de la inmigración a países desarrollados y evitar fraudes de identidad. De hecho, un proyecto de envergadura relacionado con la introducción de medidas biométricas en pasaportes en EEUU, "*Enhanced Border Control Act*", fue tractor en la estandarización y desarrollo en este campo a nivel mundial. Como consecuencia, la industria relacionada norteamericana se posicionó y la europea, tecnológicamente más avanzada, quedó como seguidora. En Europa, aunque se cuenta con la experiencia de casos destacados, los organismos competentes, como la Comisión Europea, recela aún de una implementación a gran escala con altos costes dada la falta de experiencia de esta tecnología relativamente nueva y del potencial impacto que eventuales fracasos y su divulgación puede suponer para la sociedad.

Los aspectos sociales siguen jugando un papel fundamental en este sector de aplicación, y, en algunos casos, ralentizando una implantación más masiva. La aparente falta de privacidad o de confiabilidad son factores que llegan a privilegiarse por encima de las ventajas de seguridad que la tecnología supone. Una interoperabilidad futura probada de los sistemas en el ámbito transnacional también mejoraría la percepción de los usuarios acerca de su efectividad.

En términos económicos, el mercado biométrico crece cada año y fuerza una mayor demanda de la industria implicada, de desarrolladores de soluciones, de investigadores y de usuarios finales.

1.1 Tipo de soluciones biométricas

Se conocen actualmente entre 20 y 30 tecnologías biométricas implementables, cada una con sus propias fortalezas y debilidades y con características propias que las pueden hacer más adecuadas para una aplicación u otra. Por ejemplo, aún siendo muy fiable, se ha comprobado que el reconocimiento por iris baja en desempeño para algunos colores específicos de esta membrana, además de ser cara y difícil de implementar. En el reconocimiento por huella dactilar, de uso tan extendido, esta marca física varía en función de la edad y la verificación se suele ver alterada por un mal funcionamiento de los dispositivos de captura. El reconocimiento facial es inmediato, pero subjetivo y también alterable por disfraces y complementos que el individuo puede colocarse en la cara.

Incluimos a continuación las principales características de las soluciones tecnológicas biométricas más comunes.

a. Huella dactilar

La identificación a través de la huella dactilar está plenamente extendida siendo usada durante decenas de años. Se suele considerar como una de las técnicas que mejor relación presenta en coste, disponibilidad y fiabilidad. Sin embargo, ésta última depende mucho de la calidad de la imagen registrada en el momento de entrada al sistema. Algún segmento específico de la población puede no ser hábil para utilizar esta solución (trabajadores manuales, con fisiologías especiales en la mano, con mayor humedad o sequedad…), contabilizado entre un 1% ó 2% de la población. Un aspecto importante es la coexistencia de numerosos tipos de sensores asociados con diferentes tecnologías, lo que crea un problema importante de interoperabilidad.

Esta técnica requiere que el individuo esté presente físicamente, en ocasiones se considera invasiva y todavía acarrea una imagen social negativa por la cual se asocia con prácticas policiales de identificación de sospechosos.

La suplantación de identidad en este tipo de sistemas puede ser relativamente sencilla y por ello, escáneres más avanzados miden también algún signo vital, por ejemplo, la temperatura del dedo en el momento del registro de información.

Destacamos:

- Buena aceptación en general, aunque mantiene connotaciones forenses.
- Buen desempeño, con una tasa aceptable de error.
- Bajo coste y sistemas compactos.
- Uso fácil.
- Solución probada en implementaciones a gran escala.
- Fácilmente impostable en sistemas básicos de captura de imagen dactilar.
- Problemas de utilización para algún sector específico de la población (2%).
- Problemas con el mantenimiento de los sensores.

b. Facial

Este tipo de identificación se basa en el análisis de la estructura facial del individuo registrada por una cámara midiendo distancias y relaciones entre puntos y creando un modelo que debe ser único por persona.

Las imágenes pueden ser tomadas a gran distancia y en principio no requiere de la colaboración del individuo (bajo intrusismo). En la actualidad, esta técnica ofrece menores garantías de fiabilidad debido a la posible disparidad de resultados, algunos relacionados con cambios en la fisonomía de los usuarios con el tiempo o incluso con condiciones del entorno. Aún así, el desarrollo de la tecnología se encuentra en pleno avance y presenta uno de los mayores crecimientos del mercado.

Destacamos:

- Alta aceptación de uso.
- Coste medio – alto y compacto.
- No intrusiva.
- Uso sencillo.
- Necesidad de algoritmos de tratamiento de imágenes avanzados, para alta resolución, capaces de discriminar fielmente las condiciones de variabilidad del entorno de cada imagen.
- La captura de datos es fácil de automatizar.
- Reutilización de bases de datos de imágenes faciales ya existentes, derivadas de los sistemas tradicionales de identificación (pasaportes, permisos de conducir).
- Aplicación posible en áreas amplias (estadios, aeropuertos…) a través de cámaras de vigilancia.
- Problemas de reconocimiento por variaciones en la cara (accesorios, gafas…) o edad.

c. Iris

A través del escaneo del iris, una cámara de vídeo registra una imagen del ojo de la persona desde una distancia aproximada típica de medio metro, recogiendo un modelo único que se registra. El "código iris" tras el proceso codificador genera una de las huellas más precisas de entre todas las técnicas biométricas, aunque esto supone admitir unas condiciones bastante restrictivas en la adquisición de datos (cámara específica, posición del ojo por lo general a una distancia precisa de

la cámara). Igualmente, permite reconocimientos remotos y no se considera excesivamente invasiva. Para evitar fraudes de identidad, es posible variar la luz que se utiliza forzando la reacción de la pupila.

Esta técnica asegura pocos fallos positivos, pero por el contrario requiere de mayor capacidad de almacenamiento.

Destacamos:

- Coste alto.
- Resultados muy buenos en cuanto a fiabilidad, con tasas de errores de identificación despreciables, aunque variables según los dispositivos de medida.
- Tasa creciente de crecimiento en el mercado.
- Avances que permiten el procesado del iris a distancia entre 2 y 3 metros.
- Retos pendientes en cuanto a la disponibilidad de bases de datos y la adquisición de modelos.
- Pendiente aún de algunos avances para una mayor comercialización: costes y percepciones sociales erróneas (posible daño físico para los ojos).
- Problemas registrados de identificación para personas con enfermedades oculares, como cataratas.

d. Tecnologías multimodales

La combinación de 2 ó más tecnologías biométricas en una solución integrada está teniendo un rápido desarrollo tecnológico y despliegue comercial, al aportar mayor flexibilidad y precisión. Se comprueba así una reducción de los tipos de errores comentados anteriormente, derivados del "ruido" que se introduce en la toma de datos y por cambios propios del usuario. Además, mejoran la aceptación del usuario que percibe una mayor sensación de confiabilidad.

"Según Forrester Research, la comercialización de soluciones para la gestión de la identidad a nivel mundial aumentará de 2.600 $millones en 2006 a 12.300 $millones en 2014"

La flexibilidad citada permite por ejemplo al usuario utilizar sólo una de las tecnologías biométricas del sistema en caso de estar impedido temporalmente para la otra o presentar rechazo a una de estas alternativas.

En definitiva, para el diseño de una aplicación biométrica multimodal, se deben considerar algunos aspectos:

- Tecnologías que se combinan: orientadas a los requisitos de la aplicación (desempeño, usabilidad…) y factores de partida, como recursos disponibles o costes que se están dispuestos a asumir.
- Fusión de datos: la combinación de tecnologías origina dos flujos de datos que se pueden procesar en diferentes momentos: en el momento de la adquisición, generando un único *input* de datos como resultado; en el momento de la decisión como resultado del proceso, combinando las decisiones como sistemas biométricos separados; o combinando los valores de aceptación por separado, para dar otro global que soporte la decisión.

Uno de los mayores problemas hoy en día con este tipo de soluciones tiene que ver con la disponibilidad de bases de datos multimodales, consecuencia generalmente de proyectos de I+D y con muestras de pocas modalidades biométricas (usualmente, voz y facial). El desarrollo de estas bases de datos es costoso, tanto en recursos como en tiempo, por lo que su implantación a gran

escala es complicada y, con ello, evaluar las probabilidades de éxito de este tipo de soluciones en implementaciones masivas.

Se comprueba que las tecnologías biométricas presentadas presentan beneficios y desventajas dependientes de la aplicación final. Por ello, la comparación de estas tecnologías fuera de su ámbito no es siempre adecuada, ya que no se contemplan las especificidades del sistema en su conjunto. De cualquier forma, se suelen manejar una serie de parámetros, objetivos y subjetivos en función de casos de experiencia, que permiten confrontar estas soluciones con el objetivo de predecir su emergencia o evaluar su adecuación a sistemas multimodales.

La Tabla 1 compara estos parámetros de las tecnologías biométricas consideradas en las descripciones anteriores.

	Huella	Facial	Iris	Voz
Tipo	Físico	Físico	Físico	Físico-Compor-tamiento
Método	Activo	Pasivo	Activo	Activo
Tasa de error igual (EER)	2-3.3%	4.1%	4.1 – 4.96%	0.1 – 0.86%
Tasa de falsa aceptación (FAR)	2.5%	4%	6%	0.75%
Tasa de falso rechazo (FRR)	0.1%	10%	0.001%	0.75%
Fallo en el registro	4%	-0%	4.1 – 4.6%	0.1 – 0.86%
Coste	Medio	Alto	Muy alto	Medio - bajo
Aceptación social	Media	Alta	Baja	Alta

Tabla 1. Comparativa tecnologías biométricas. Fuentes: Opus Research, European Comission, IPTS.

A raíz de esta comparativa, la tecnología biométrica vocal ofrece unas posibilidades más que atractivas, con datos de fiabilidad probados, percepción social favorable y bajo grado de intrusismo, facilidad de uso e interacción, y coste bajo comparativo de implantación.

1.2 Sectores de aplicación

La aplicación de la biometría abarca variados sectores de actividad e impacta desde diferentes perspectivas en el beneficio de la sociedad. A nivel nacional o transnacional, es un mecanismo efectivo para el control de pasos fronterizos, mejorar la seguridad de las redes de computación, prevenir fraudes financieros, controlar el acceso físico a servicios o instalaciones, o verificar la asistencia y tiempos. A nivel de consumidor, la biometría es una alternativa efectiva para preservar la identidad de la persona y prevenir el fraude por suplantación.

Se reconocen aquí los siguientes sectores de aplicación biométrica:

a. Control de fronteras e inmigración

La autentificación de la identidad de viajeros en los controles de frontera es un medio esencial para reforzar la seguridad o para la detección de la inmigración ilegal. En un futuro cercano, la mayor parte de los países requerirán de sus ciudadanos que presenten una prueba biométrica para el paso fronterizo, de entrada y de salida. En este sentido, la implantación de sistemas basadas en el escaneo de huellas dactilares y reconocimiento de iris están siendo las soluciones más frecuentes, fundamentalmente en los aeropuertos.

b. Entorno aeroportuario

Las tecnologías biométricas se han implantado con éxito en algunos de los mayores aeropuertos del mundo, mejorando las condiciones de seguridad y productividad. La autentificación a las zonas de cabinas de aviones, equipajes, áreas de embargue o de mantenimiento está ya regulada por soluciones de este tipo. En este entorno, no sólo las aplicaciones biométricas permiten verificar el paso autorizado de pasajeros, sino que puede regular el paso de los empleados a zonas restringidas o detectar la entrada de criminales al aeropuerto.

En este sector del transporte aéreo, ICAO (*International Civil Aviation Organization* **¡Error! No se encuentra el origen de la referencia.**) ha trabajado en el establecimiento de una serie de estándares internacionales orientados a la industria y se postula por el reconocimiento facial como principal tecnología biométrica, seguida del escáneo de iris y de huella dactilar como complementarias a la primera. La prioridad por mejorar las condiciones de seguridad en los vuelos comerciales ha crecido año tras año sobre todo tras los atentados terroristas del 9/11. Se estima que la aplicación para este control de viajeros es aún pequeña en cuota de mercado dentro del sector biométrico (2%), pero con un crecimiento anual cercano al 50%.

Según una encuesta realizado por la empresa SITA, proveedor de soluciones TIC para el sector del transporte aéreo, a 129 aerolíneas, el 20% de éstas están invirtiendo recursos en integrar soluciones biométricas en sus operativas de viaje.

c. Control de acceso físico a zonas restringidas

Uno de los usos más extendidos de la biometría es el del control de acceso físico a edificios o zonas restringidas por motivos de alta seguridad. Por esta necesidad de mayor restricción, se utilizan varias tecnologías biométricas, por separado o en combinación, para asegurar la entrada del personal autorizado según diferentes grados de permisos.

d. Servicios bancarios

"Un tercio de los clientes encuestados para un estudio de Alcatel-Lucent optarían por un banco con medidas de seguridad basadas en biometría de voz"

La aplicación de soluciones biométricas para servicios financieros, comercio electrónico y pagos móviles cuenta con una estimación alta de crecimiento anual, en torno al 21%, y una cuota de mercado sobre el ámbito biométrico global del 14%. El robo de identidad digital para fraudes financieros es el delito de guante blanco con una incidencia cada vez mayor y las entidades bancarias tienen una prioridad en mejorar la autentificación de las identidades para asegurar las transacciones.

Esto es aplicable por ejemplo al acceso de cajeros automáticos, banca on-line o autentificación de la identidad del punto de venta. De especial interés para la biometría vocal resulta su aplicación en banca móvil y autentificación por voz.

Ante esta perspectiva, la securización de la información y de la identidad en transacciones realizadas por dispositivos móviles es clave para vencer la desconfianza de los usuarios en los métodos habituales de seguridad de sus bancos. Una investigación de mercado realizada por las empresas Alcatel Lucent y SpeechStorm con encuestas a un panel de clientes durante 2008 ofrece datos interesantes que corroboran el hecho de que los bancos y responsables financieros deben ser mucho más activos a la hora de adoptar tecnologías que mejoren la seguridad de sus servicios. Un 79% de los encuestados estarían dispuestos a utilizar en un futuro cercano la biometría vocal para acceder a servicios bancarios. Un 38% optaría por ser cliente de un banco que mejore las condiciones de seguridad por biometría de voz respecto de otro que no. Incluso un 37% de ellos estaría dispuesto a pagar una pequeña tasa adicional como cliente de un banco que invierta en optimizar la seguridad de sus operativas.

A través de diferentes medios de comunicación y foros, empresas tan relevantes como Barclays o HSBC se han posicionado públicamente interesados en el potencial que la biometría de voz puede significar para ofrecer servicios más rápidos y seguros a sus clientes.

e. Administraciones públicas e identificación civil

La aplicación de las tecnologías biométricas por parte de gobiernos y administraciones públicas constituye aún el mayor mercado vertical. El caso concreto de aplicación en identificación civil mantiene una tasa de crecimiento anual del 29%, suponiendo ahora una cuota del 40% respecto del mercado global de la biometría. Esta necesidad de mayor eficiencia y seguridad en la identificación de los ciudadanos se ha traducido en números programas ya ejecutados o en marcha para la utilización de e-pasaportes, e-ID, visados o votos electrónicos. Como referencia, se puede destacar que a principios de 2011, 90 países de todo el mundo contarán con programas de pasaportes electrónicos, lo que supone un desafío en términos de interoperabilidad internacional. Se prevé que en 2014, Asia supere a Europa en número de e-pasaportes expedidos. Aquí, con poblaciones y economías en emergencia, se conocen casos de éxitos de gran envergadura. En la India, el gobierno implantó una solución biométrica multimodal (facial y huella dactilar) para evitar el fraude por cambio de identidad a la hora de solicitar la tarjeta nacional de identidad. En Oriente Medio, en los estados petrolíferos, el reconocimiento de iris es una tecnología cada vez más en uso para la identificación de trabajadores extranjeros. Mediante este procedimiento, en los Emiratos Árabes Unidos han detectado y expulsado a más de 300.000 personas que habían entrado en el país ilegalmente.

f. Verificación de identidad electrónica

La securización en las comunicaciones es esencial para diferentes sectores de la sociedad (legal, financiero, militar). Esta información, que se envía por canales y formatos diferentes (texto, imagen, voz) debe contrastarse, tanto como contenido válido como fuente original segura. Para ello, estos datos pueden ser validados incluyendo una medida biométrica del emisor y validándola contra una base de datos de personal autentificado. Tecnologías biométricas como huella dactilar, facial, iris, voz o combinación multimodal puede adaptarse para esto. En concreto, la información transmitida sobre un canal de audio puede verificarse incorporando un software de reconocimiento en el receptor y contrastándolo con un conjunto de modelos de personas conocidas.

Según *Secure Enterprise Magazine*, un usuario medio maneja hasta 8 contraseñas, en formato de texto o numérico tipo PIN. El 55% de éstos escriben al menos una de estas contraseñas y un 9%, todas. La biometría vocal puede solucionar sin duda los evidentes riesgos de seguridad que estas prácticas suponen.

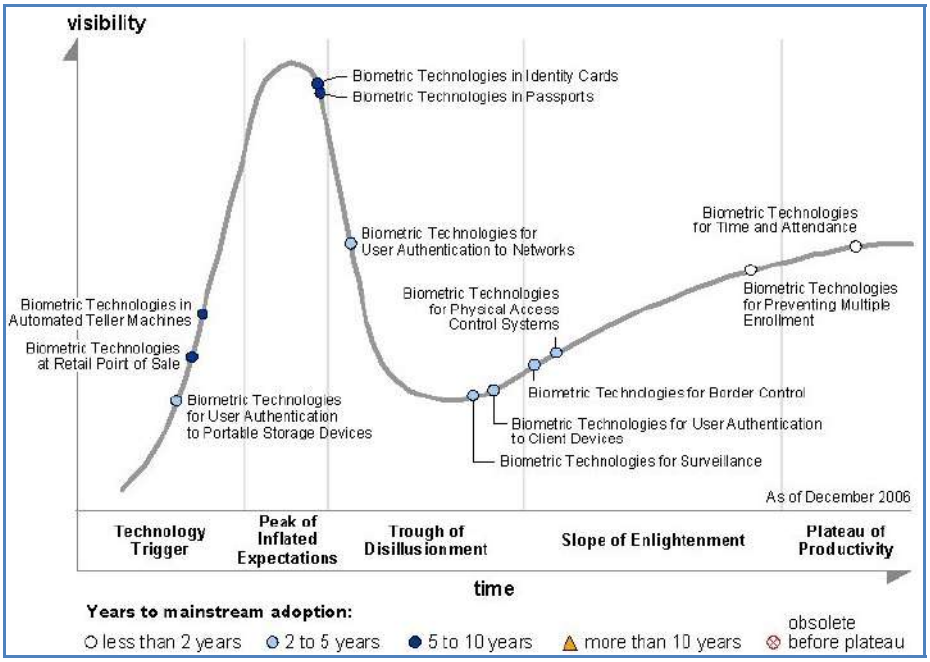


Figura 1. Curva de estimación *hype-cycle* sobre aplicaciones biométricas. Fuente: Gartner Group.

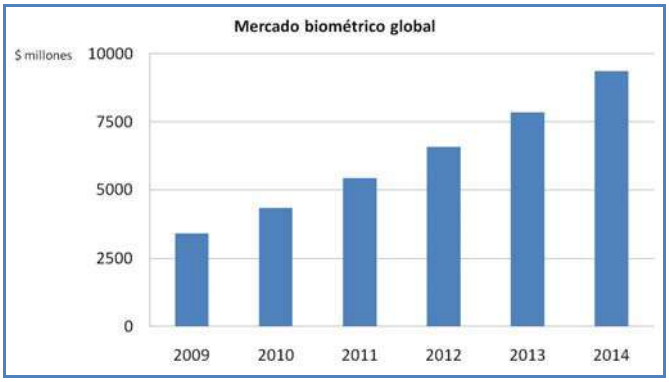
Resulta interesante comprobar el tipo de soluciones que este análisis sitúa como disruptivas tecnológicamente y que más están atrayendo la atención de la industria, siempre, en el año 2007 de publicación. Destacan aquí la aplicación de la biometría en cajeros automáticos de bancos o terminales de venta de productos, con una adopción comercial prevista en un plazo de 5-10 años.

1.3 Potencial de mercado

En el pasado más reciente, el mercado de la biometría se ha centrado casi exclusivamente en tres tipos de aplicaciones. Por un lado, el control de acceso físico dominó el mercado biométrico (42% a principios de 2000), seguido de la incorporación en aplicaciones TI, como portátiles o como interfaces de acceso específicos (25%). Por último, el tercer mayor sector era el de los servicios financieros (15%), el más dado a evolucionar rápidamente debido a la nueva gestión de la identidad digital, los nuevos tipos de fraudes o los cambios en el concepto de banca en sí.

La demanda de soluciones biométricas ha cambiado en función de nuevas necesidades de seguridad y los avances tecnológicos. El sector público y las administraciones protagonizan esta evolución, liderando el sector por volumen y centrando el foco en cuestiones de seguridad nacional, transporte, inmigración e interoperabilidad a gran escala.

Siempre según datos de IBG (*International Biometrics Group)*, empresa consultora y de investigación de mercado específica de este sector, se prevé una evolución del volumen del mercado biométrico global con tasas de crecimiento lineales durante los próximos años (Figura 2). Esto supone una tasa de crecimiento anual compuesto (CAGR) del 22.3%.



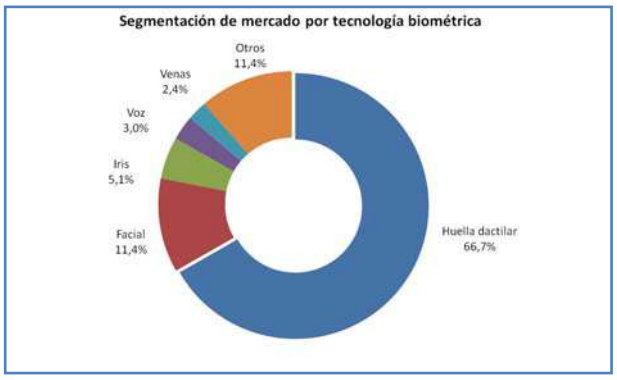


Figura 2. Volumen y evolución del mercado biométrico global; segmentación de mercado por tecnología (2009). Fuente: IBG.

[M$]	2009	2010	2011	2012	2013	2014
Dactilar	2.280	2.869	3.556	4.218	4.947	5.792
Facial	390	510	675	848	1.097	1.417
Iris	174	288	361	480	578	730
Voz	104	109	113	136	167	189

Figura 3. Evolución del volumen de mercado por tecnologías biométricas. Fuente: IBG.

"La demanda del sector público en torno a la gestión de la identidad liderará la evolución futura de este mercado"

Este aumento previsto del mercado tiene en efecto el impulso principal de programas de gestión de la identidad de gobiernos de todo el mundo y sistemas de gestión de fronteras. EEUU y el sudeste asiático son los principales mercados actuales en productos y servicios relacionados, mientras las economías emergentes de Asia, Oriente Medio y África ganarán protagonismo por programas ya en marcha o previstos en un plazo de 2 ó 3 años.

La Figura 3 incluye una estimación de la segmentación del mercado actual de la biometría según el tipo de tecnología utilizada, con un dominio claro de las soluciones basadas en reconocimiento de huella dactilar, fundamentalmente de sistemas tipo AFIS (*Automated Fingerprint Identification System*). Esta tecnología es de las más antiguas técnicas biométricas, impulsada por la demanda de los organismos legales y policiales para la identificación. Su amplia extensión se ha debido a un buen balance de factores como universalidad, muestras permanentes y distintivas, desempeño, aceptación, bajo coste de lectores… La utilización única de esta tecnología compromete sin embargo el acceso universal y una disponibilidad permanente en aplicaciones a gran escala, además de estar expuesta fácilmente a suplantaciones de identidad.

El escenario de volumen de mercado para aplicaciones biométricas por voz es prometedor, casi duplicándose en un plazo de 4 años y con una tendencia aun más creciente a partir de 2011.

Ya hemos destacado que la gestión de la identidad con fines civiles y de identificación criminal será uno de los principales campos de aplicación motores del sector. La prospectiva de mercado de IBG confirma este escenario, en el que las aplicaciones para la identificación civil tienen una creciente demanda impulsadas por los programas de seguridad para el control de fronteras. Según este estudio, con datos analizados de 2008, las empresas Cogent Systems (recientemente adquirida por 3M), CrossMatch, Motorola y Sagem son las líderes en este subsector con unas cuotas de mercado del 7.5%, 5.3%, 5% y 2.8%, respectivamente.

En el ámbito del control de acceso físico y de la asistencia (Figura 4), la estimación comercial también plantea un crecimiento en el volumen de mercado asociado, aunque no tan relevante como el anterior de la gestión de la identidad en el campo civil. Aquí, Suprema (6.9%), Bioscrypt L-1 (6.8%) y Nitgen (2.3%) son las principales empresas proveedoras de soluciones.

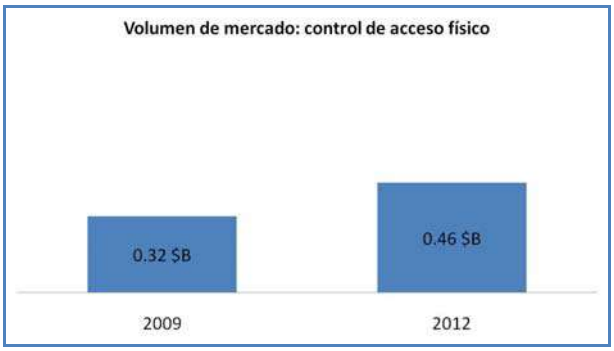


Figura 4. Evolución del volumen de mercado en el ámbito del control de acceso físico. Fuente: IBG.

El desarrollo actual y futuro del sector global biométrico viene determinado por una serie de factores de cuya evolución dependerá una implantación más masiva y exitosa:

- ✓ Los nuevos desafíos globales de seguridad y alerta anti-terrorista crearon unas expectativas desmedidas acerca de la necesidad ya inminente de mejorar las condiciones de seguridad mediante tecnologías biométricas. Sin embargo, esta aceleración no fue paralela con el grado de aceptación que mostraba el mercado.
- ✓ Durante años, se ha difundido sobre la biometría un mensaje de tecnología disruptiva a punto de ser explotada comercial y masivamente que no se ha llegado a materializar. Esto ha generado desconfianza por parte de la industria a la hora de apostar por nuevos avances tecnológicos. En el pasado, el foco se ha centrado en el desempeño de las soluciones cuando la base tecnológica no se había desarrollado plenamente para ofrecer toda su potencialidad. También, el entorno de implantación de las aplicaciones no ha sido siempre el adecuado para dar a conocer todas las posibilidades de la tecnología y atraer así a usuarios e industria.
- ✓ Una prueba definitiva para conocer el grado de madurez de este tipo de soluciones pasa por la puesta en marcha de grandes sistemas biométricos en el sector público. Se trata en general de programas de progresos lentos, con retrasos en su ejecución o en pleno desarrollo. Se han nombrado ya algunos de ellos: FBI-NGI (*Next Generation Identification*), NBIS (*UK National Biometric Identity Service*), EU VIS (*European Visa Information System*).
- ✓ El sector industrial especializado se ha caracterizado recientemente por adquisiciones y fusiones entre sus principales actores. Por ejemplo:
  - Digimarc y Bioscript, por L-1.

- Printrak (Motorola Biometrics) por Sagem.
- Cogent Systems, por 3M.
- Labcal, por Cross Match.

✓ Esfuerzo en la estandarización que mejore la interoperabilidad e integración de las soluciones. ISO (*International Organization for Standardization*) **¡Error! No se encuentra el origen de la referencia.** trabaja en el desarrollo de más de 60 estándares que apoye la integración del equipamiento biométrico durante los próximos años. Actualmente, la mayoría de las soluciones en funcionamiento se forman con componentes heterogéneos cuya integración entre ellas supone un coste adicional de adaptación, tiempo y riesgo en el desempeño.

✓ Esfuerzo por comprender mejor la aceptación de los usuarios antes estas soluciones (barreras en el uso, intrusismo, confidencialidad, facilidad y flexibilidad, ubicuidad…).

✓ La evolución del mercado biométrico debe ir apoyada por una evolución de conceptos a nivel tecnológico, de aplicación y de usuario.

- Frente a un despliegue limitado, hacia una mayor ubicuidad y coberturas más amplias.
- Frente a unos costes elevados de implantación, hacia una mejor relación coste/desempeño.
- Frente a sistemas rígidos en cuanto a su utilización, a formas más flexibles y dinámicas.
- Frente a una dependencia de algoritmos y formatos, hacia una mayor interoperabilidad.
- Frente a una actitud proactiva del usuario hacia otra más pasiva.

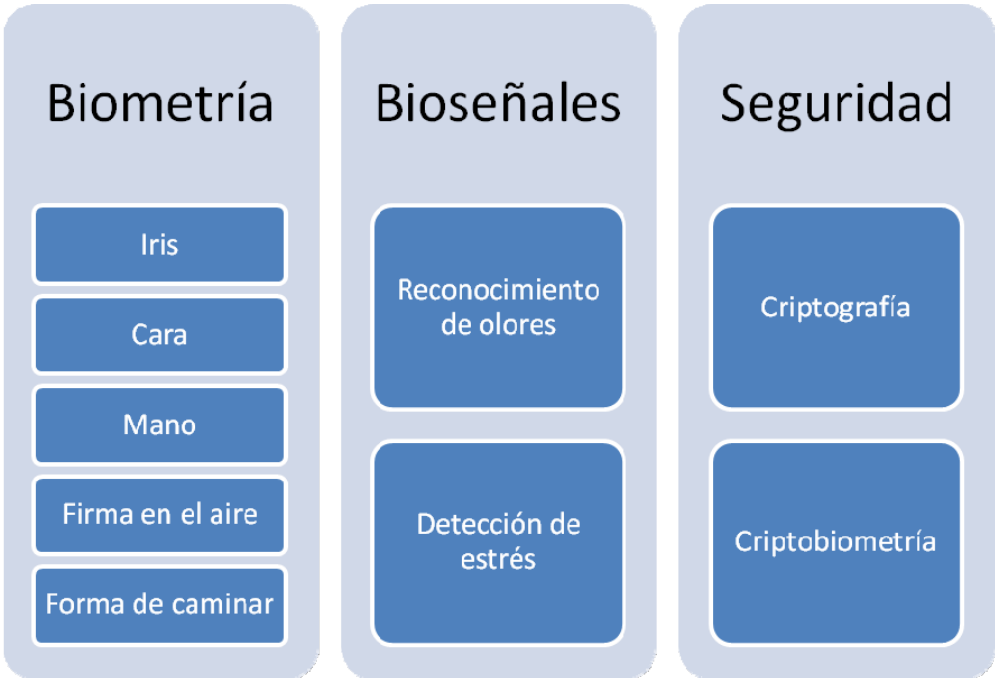
Frente a sistemas biométricos específicos por proyectos, hacia una cartera de servicios biométricos más flexibles. En este sentido, los proveedores de soluciones de gestión de la identidad optarán por descomponer sus productos siguiendo el paradigma SOA de arquitecturas distribuidas de servicios, dando forma al concepto IAAS (*identity-as-a-service*).

2. Capacidades I+D y soluciones tecnológicas UPM – Biometría

Se detalla información de las capacidades de I+D, líneas de actividad y soluciones tecnológicas desarrolladas por la UPM:

2.1 GB2S (Grupo de Biometría, Bioseñales y Seguridad) – Centro de I+D CeDInt

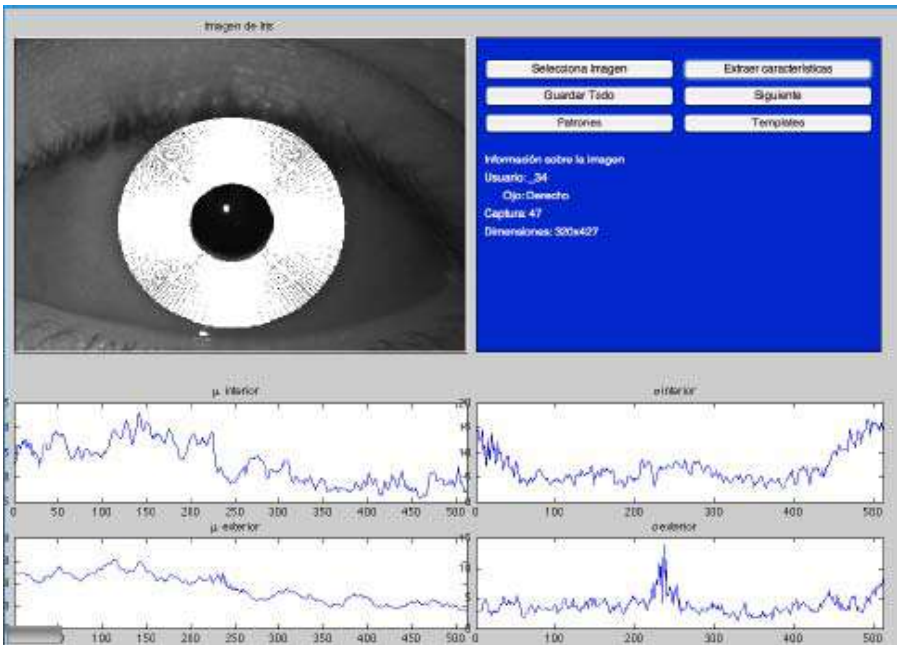
2.1.1 Líneas de actividad



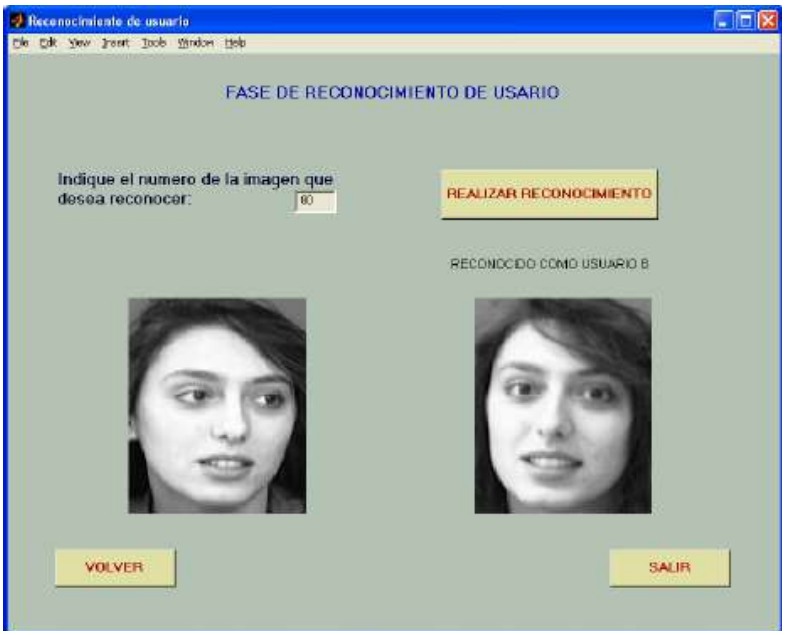
- **BIOMETRÍA**

  Desarrollo tecnológico e investigador centrado fundamentalmente en las siguientes técnicas biométricas:

  - **Iris**: foco no sólo en el área de la identificación sino también en el de la impostación con el objetivo de mejorar los niveles de seguridad globales de este tipo de sistemas. Aplicación de algoritmos biométricos para iris a aplicaciones móviles.
    - Segmentación, extracción de caracteres, comparación de patrones.
    - Foco en entornos móviles.
    - Antifalsificación: ataques a sistemas de iris, falsificaciones de texturas, ataque canal lateral.

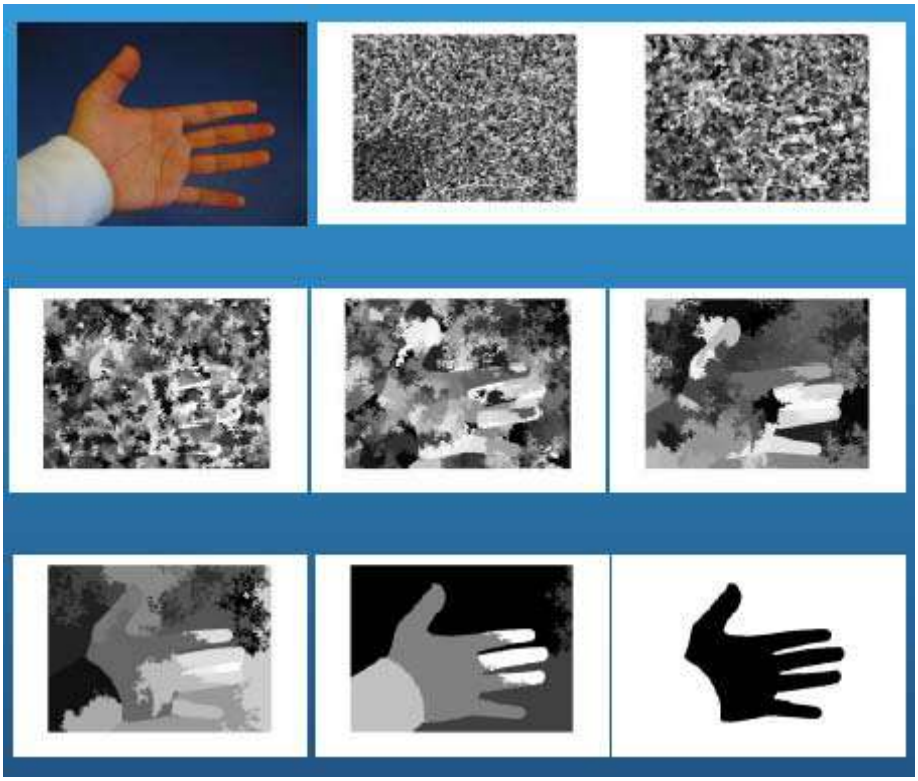


- **Reconocimiento facial:** objetivos centrados en proveer técnicas biométricas basadas en la identificación de individuos por rasgos faciales. Foco en proveer aplicaciones de uso diario vía PC y dispositivos móviles.
  - Segmentación, extracción de características y clasificación de usuarios.
  - Imágenes baja calidad. Procesamiento en vídeo.
  - Detección de cara natural. Clasificación de edad.



- **Geometría de la mano:** fusión de algoritmos de reconocimientos de huella de la mano y geometría para la identificación final e incremento de tasas de aceptación, en entorno no invasivos.

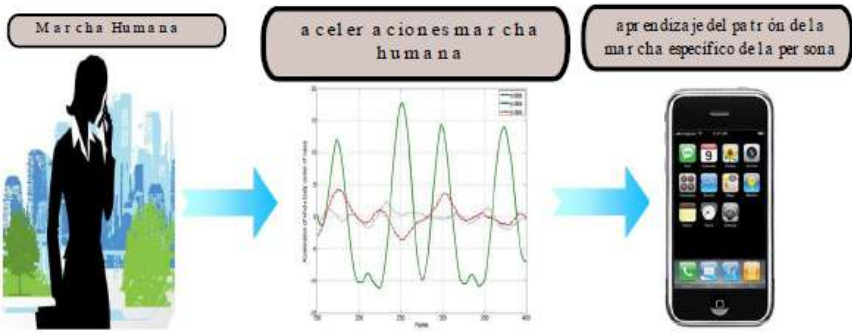
- Gran aceptación de usuario, no invasivo. Invariante a rotación.
- Foco en dispositivos móviles y bases de datos.
- Fusión con Palmprint. Mejora seguridad en móviles.



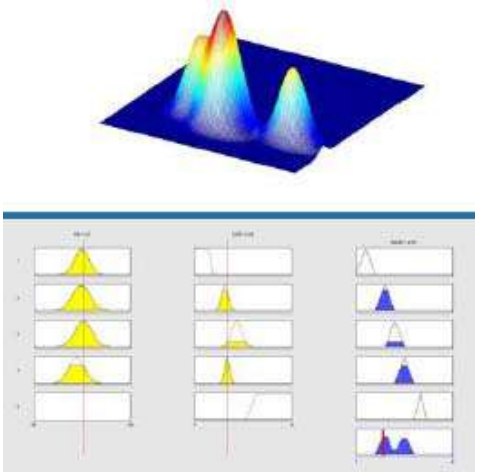
- **Firma en el aire**: desarrollo de técnica de firma en el aire en base al análisis del gesto en el aire utilizando un dispositivo con un acelerómetro incluido (posibilidad de utilización de un dispositivo móvil). Know-how adquirido en técnicas biométricas de reconocimiento de gestos.
  - Idea innovadora.
  - Dispositivos móviles, bases de datos, estudio de falsificaciones.
  - Aplicaciones en seguridad, control de interfaces y videojuegos.

Más información: http://www.madrimasd.org/informacionidi/noticias/noticia.asp?id=50675

- **Cadencia de paso**: identificación a través de la forma de los movimientos y características de paso de los individuos, alcanzando tasas de error aceptables.
  - Reconocimiento de la forma de caminar (característica intrínseca de cada individuo). Acelerómetros.
  - Dispositivos móviles y dispositivos orientados y específicos.
  - Aplicación a la detección de robo del dispositivo móvil.



- **BIOSEÑALES:**
  - **Detección de estrés:** los sistemas biométricos aseguran altos niveles de seguridad para el acceso físico, pero no pueden evitar que los propios individuos sea utilizados como "llaves" para acceder al sistema. Por lo tanto, el sistema de detección de estrés es una solución para determinar el estado psíquico-físico de los individuos y conocer información de su contorno (por ejemplo, si la persona está siendo coaccionada para acceder a un sistema o entorno).
    - Detección de estrés a través de señales fisiológicas (conductancia de la piel, tasa cardíaca) y lógica difusa.
    - Detección en tiempo real.
    - Posibilidad de incluir más factores.
    - Aplicaciones: biometría, medicina y salud, entrenamiento en simuladores.



  - **Análisis del olor humano:** técnica de aplicación biométrica basada en el reconocimiento del olor único de cada persona, independiente de cualquier producto químico de uso corporal. Se pretende reconocer a cada persona basado en un patrón químico único, con aplicaciones posibles desde la identificación en aeropuertos o la detección de componentes químicos en la piel humana.
    - Biomarcadores, espectrogramas de masas.
    - Análisis de picos en espectrogramas; aliento y sustancias en piel; complejidad de extracción.
    - Aplicaciones en biometría, detección de enfermedades y explosivos.

- **SEGURIDAD, CRIPTOGRAFÍA Y CRIPTOBIOMETRÍA:**
  - **Criptografía y criptobiometría:**
    - Protocolos de seguridad, criptográficos, funciones hash.
    - Criptobiometría: biometría + criptografía.
    - Aplicaciones de seguridad.

2.1.2 Soluciones tecnológicas

- Método para la cuantificación del estrés en un usuario.
  - Sistema protegido por patente (Referencia: EP11382327.2).
  - Titularidad patente: UPM (100%).
  - Inventores UPM: Carmen Sánchez Ávila, Alberto de Santos Sierra, Gonzalo Bailador Pozo, Javier Guerra Casanova, Vicente Jara Vera, Centro de I+D CeDInt.
  - Descripción: método para la cuantificación del estrés en un usuario donde dicho método permite establecer una discriminación entre usuarios con estrés y usuarios relajados. El patrón de estrés comprende valores medios de tasa cardíaca y respuesta galvánica de piel. Permite la detección de estrés de una forma no invasiva y un sistema inteligente decisor para el control de acceso físico.
- Dispositivo y método de detección de estrés mediante señales fisiológicas.
  - Sistema protegido por patente (Referencia: P200930993).
  - Titularidad patente: UPM (50%), Secuware (50%).
  - Inventores UPM: Carmen Sánchez Ávila, Alberto de Santos Sierra, Javier Guerra Casanova, Centro de I+D CeDInt.
  - Descripción: dispositivo y método de detección de estrés mediante señales fisiológicas que comprende una etapa de enrolamiento y una etapa de acceso. Este dispositivo, no invasivo e integrable en cualquier sistema de acceso con identificación biométrica, tiene aplicación directa en el campo de la seguridad, como en el control de accesos a edificios y servicios o la seguridad informática.
- Sistema de reconocimiento biométrico basado en geometría de mano sin contacto en dispositivos móviles.
  - Sistema protegido por patente (Referencia: PCT/ES2011/070792).
  - Titularidad patente: UPM (100%).
  - Inventores UPM: Carmen Sánchez Ávila, Alberto de Santos Sierra, Centro de I+D CeDInt.
  - Descripción: sistema biométrico de reconocimiento de usuarios basado en la información del contorno de la mano aplicando técnicas de tratamiento de imágenes, para generar unos parámetros descriptores que contienen la información necesaria que se asocia con un individuo particular. De esta manera es posible identificar unívocamente a una persona y realizar comparaciones entre distintas imágenes que pueden o no corresponder con diferentes usuarios. La aplicación directa más inmediata se orienta hacia la identificación del usuario para el acceso a móvil o PC con cámara digital integrada sin la necesidad de introducir un código PIN.

- Sistema biométricos desarrollados a través de:
  - Reconocimiento de iris;
  - Reconocimiento facial;
  - Reconocimiento por firma en el aire con dispositivo móvil.

2.2 Departamento de Tecnología Fotónica y Bioingeniería – ETSI Telecomunicación / Facultad de Informática

2.2.1 Líneas de actividad

- Visión artificial
- Procesamiento paralelo
- Procesado borroso

2.2.2 Soluciones tecnológicas

- Sistema de detección y verificación de identidad de personas a través de rasgos faciales.
  - Sistema protegido por patente (Referencia: P200500912)
  - Titularidad patente: Universidad Rey Juan Carlos de Madrid (80%) y UPM (20%).
  - Inventores UPM: Jorge Antonio Ruiz Mayor, Facultad de Informática.
  - Descripción: sistema de detección y verificación de la identidad de personas a través de sus rasgos faciales. El problema de verificación de caras humanas se puede sintetizar como la tarea de comprobar si un nombre dado coincide con un rostro observado, utilizando únicamente los rasgos faciales, sin utilizar otros elementos (voz, huellas dactilares, firma, ADN, etc.). Combina el reconocimiento automático de la cara del individuo con la comprobación de un código personal.

2.3 Departamento de Arquitectura y Tecnología de Sistemas Informáticos (DATSI) – Facultad de Informática

Grupo de I+D: Informática Aplicada al Procesado de Señal e Imagen

2.3.1 Líneas de actividad

- Tratamiento de la señal de voz
- Bioinformática
- Aplicaciones del tratamiento de la voz y la identificación del locutor en entornos de seguridad
- Teledetección

2.3.2 Soluciones tecnológicas

- Método y sistema para la estimación de parámetros fisiológicos de la fonación y su aplicación clínica y biométrica.
  - Sistema protegido por patente (Referencia: P201131069)
  - Titularidad patente: UPM (100%)
  - Inventores UPM: Pedro Gómez Vilda, Victoria Rodellar Biarge, Víctor Nieto Lluis, Rafael Martínez Olalla, Agustín Álvarez Marquina, Facultad de Informática.

- Descripción: método y sistema de cómputo para el registro y análisis de la voz, que permite calcular una serie de parámetros de la fonación. Estos transportan información relevante sobre influencias causadas por trastornos orgánicos (que afectan a la fisiología de la laringe) o neurológicos (que afectan a los centros cerebrales del habla). Asimismo se consideran parte esencial de la invención los procedimientos clasificatorios que permiten obtener estimaciones de la disfunción presente y de asignación de personalidad. La utilidad de la invención se enmarca, en la posibilidad de aplicar la estimación de disfunción en los centros médicos de asistencia primaria para el cribado de pacientes a los centros de atención especializada, simplificando los protocolos de exploración, ahorrando costes, y reduciendo listas de espera. También es aplicable esta metodología en la detección de la personalidad del locutor por la voz, permitiendo garantizar el acceso a instalaciones o servicios.

- Glottex Voice Analysis System
  - Software registrado en el Registro de la Propiedad Intelectual de Madrid (Referencia: M-006038/2008)
  - Descripción: aplicación software para el análisis avanzado de la voz y la determinación de la muestra más cercana a la huella vocal biométrica. Esta nueva solución identifica con mucha mayor fiabilidad rasgos únicos de la voz, distinguiendo aquellos que se derivan del tracto vocal (faringe, cavidad oral, cavidad nasal) de los propios de la fuente de excitación origen de la voz. Como aplicación biométrica, aporta mayor fiabilidad en la identificación del locutor, una adaptación sencilla y de bajo coste de la herramienta biométrica a la infraestructura de voz ya existente y la posibilidad de identificación remota.

3. Empresas UPM – Biometría

Se detalla información sobre empresas apoyadas por el Programa de Creación de Empresas UPM relacionadas con el ámbito de la biometría:

3.1 Agnitio

Empresa que desarrolla productos para la gestión y verificación de identidades. La tecnología biométrica de Agnitio permite erradicar fraudes de identidad en transacciones remotas (vía telefónica o Internet) sin necesidad de nuevos dispositivos. Los productos de Agnitio son el resultado de la combinación de una tecnología puntera y 10 años de colaboración con departamentos de seguridad del estado. Organizaciones policiales y de inteligencia en tres continentes usan ya estos productis en sus actividades diarias en más de 20 idiomas distintos.

Agnitio es una empresa constituida a partir del Área de Tratamiento de Voz y Señal (ATVS) de la E.U.I.T. Telecomunicaciones de la Universidad Politécnica de Madrid.

Web: http://www.agnitio.es

3.2 Biometro Soft

Empresa que se orienta a la comercialización, desarrollo e investigación de nuevas técnicas, metodologías y productos orientados a la evaluación y análisis de la voz, basados en la onda glótica, con aplicación clínica, forense y biométrica. Los productos de esta compañía poseen un elevado valor social, caracterizándose por su elevada fiabilidad, no ser invasivos, bajo coste y rápida ejecución.

Biometro Soft S.L. es una empresa constituida a partir del Grupo de Investigación GIAPSI de la Facultad de Informática de la Universidad Politécnica de Madrid.