XXVII Convocatoria 2006 de Premios

"Ingenieros de Telecomunicación"

Premio *BANESTO* al Mejor Proyecto Fin de Carrera en *Tecnologías de la Información y las Comunicaciones en la Banca*

Proyecto Fin de Carrera:

Identificación Biométrica en Dispositivos Integrados

Paloma Ferruelo Soler

-

Origen

El Proyecto Fin de Carrera surge en el seno del Grupo de Diseño Microelectrónico y Aplicaciones (DMA), adscrito al Departamento de Tecnología Electrónica de la Universidad Carlos III de Madrid. Más concretamente, se originó en el subgrupo especializado en el sector de Tarjetas Inteligentes y la Biometría, conocido como *Grupo Universitario de Tarjeta Inteligente (GUTI).*

En dicho grupo se trabaja continuamente en mejorar las prestaciones de los Sistemas de Identificación, prestando especial atención al incremento de necesidades de seguridad que se requieren en multitud de ámbitos en nuestro entorno.

Gracias a los avances y al amplio conocimiento del GUTI en el campo de los Sistemas de Identificación Biométrica y sus trabajos con Tarjetas Inteligentes (sistemas Match-on-Card), se observó una posibilidad de combinar ambas técnicas para la obtención de sistemas con mayor nivel de seguridad. En concreto se optó por la implementación de soluciones de identificación personal portátiles de altas prestaciones, para su potencial aplicación a sistemas de seguridad y banca.

Se barajaron distintas alternativas, para que en un futuro pudiera llevarse a cabo la implementación en distintas plataformas, tales como una tarjeta inteligente, o un Token USB.

Se decidió emplear el iris ocular como técnica de reconocimiento biométrico para el sistema a desarrollar. Esta modalidad biométrica ofrece múltiples virtudes y, a pesar de ser una técnica relativamente reciente y menos consolidada que las basadas en huellas dactilares, ofrece una fiabilidad equivalente o incluso superior.

Objetivos

Se decidió, por tanto, implementar un sistema de autenticación biométrica basado en el reconocimiento del iris ocular. Al tratarse de un sistema de verificación, cada usuario tendrá su patrón almacenado en su propio dispositivo portátil (Token) y sólo será necesario comparar la muestra adquirida con este patrón, cuando el individuo desee autenticarse ante el sistema.

Esta solución utiliza un microcontrolador de altas prestaciones como soporte para realizar las principales tareas del sistema, con el objetivo de incrementar la carga de procesamiento en el dispositivo portátil.

El objetivo principal es que el microcontrolador realice la mayor parte del proceso, de forma que se eliminen los agujeros de seguridad potencialmente existentes en los ordenadores y/o terminales donde se quiera autenticar el usuario. Se incluye en el proyecto un análisis de las técnicas de identificación más comunes, para elegir aquellos algoritmos que requieran menos recursos (memoria, capacidad de proceso, etc.), y que por tanto, resulten más idóneos para su implementación en el microcontrolador.

Desarrollo

Para conseguir desarrollar el sistema descrito anteriormente se consideraron necesarios tres elementos fundamentales:

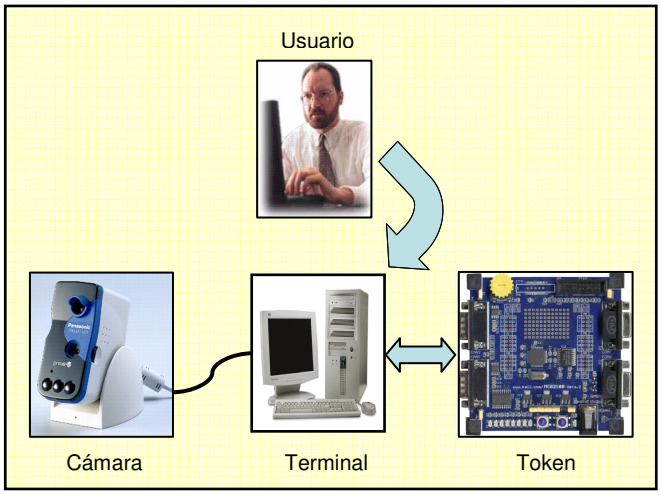

Figura1: Elementos del sistema

- **Cámara:** La cámara es la encargada de capturar la imagen del usuario, tras lo cual transfiere dicha información al terminal para su preprocesado.
- **Terminal:** Es el dispositivo que actúa como interfaz con el usuario y realiza alguna de las funciones del sistema biométrico.
- **Token:** Representa el dispositivo integrado y se encarga de completar el proceso de identificación.

Para facilitar el proceso se decidió abordar el problema gradualmente y estructurar su desarrollo en tres versiones, de forma que en la primera de ellas el microprocesador se encargara únicamente de realizar las últimas etapas de la identificación. Mientras que en la última versión (versión 3), se encargase de realizar todas las tareas de la identificación excepto el preprocesado de la imagen, de lo cual siempre se encarga el Terminal.

Este tipo de sistemas se componen de dos procesos principales basados en la función que desea realizar el usuario:

- **Reclutamiento en el sistema:** consiste en tomar la imagen del usuario, obtener su patrón característico y almacenarlo en memoria para posteriores verificaciones. Esta es la primera operación que debe realizarse para poder hacer uso de este tipo de aplicaciones.
- **Verificación:** Similar a la anterior, excepto que una vez obtenido el vector característico del individuo se compara con el almacenado anteriormente. Como resultado de esa comparación, se permite o deniega el acceso del usuario en el sistema.

En la figura siguiente se muestran las etapas que constituyen estas operaciones. A continuación se describirán brevemente cada una de ellas y cómo se han implementado en el sistema desarrollado.

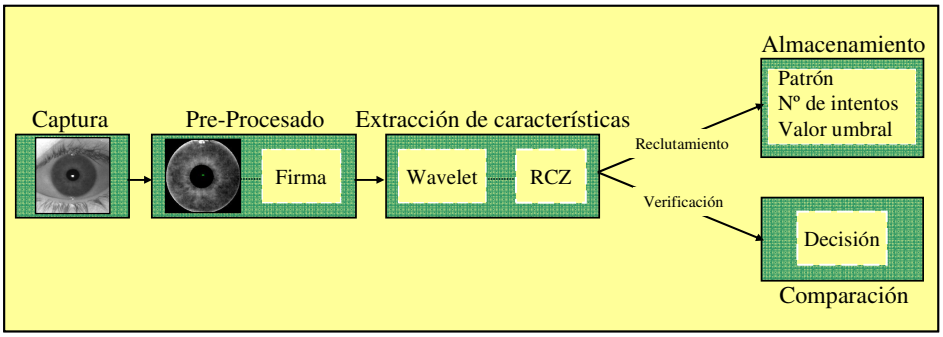

Figura 2: Fases del proceso de autenticación

1. **Captura de datos:** La captura de los datos se realiza a través de una cámara. El procedimiento a seguir es muy sencillo ya que el usuario debe mirar fijamente a la cámara desde una distancia aproximada de 50 cm y cuenta con la ayuda de una señal luminosa que le ayuda a posicionarse correctamente.
2. **Preprocesado:** Esta etapa es la encargada de adecuar la imagen capturada, eliminando de ella todos los puntos irrelevantes, es decir aquellos que no forman parte del iris. De esta nueva imagen se obtiene la firma del iris, o conjunto de datos que describe la identidad del usuario. El preprocesado se divide en dos bloques principales:
    a. **Localización del iris:** Se centra en la obtención de dos circunferencias que definan el contorno exterior e interior del iris. Estas circunferencias coinciden con aquellas que presentan máximo gradiente de intensidad en la escala de grises de la imagen.
    b. **Cálculo de la firma:** La firma es una señal unidimensional que contiene la información necesaria para la correcta extracción de características del sujeto. En este caso, la firma se construye a partir de 256 valores de intensidad de gris, resultado de muestrear una circunferencia ubicada entre los bordes anteriormente localizados.
3. **Extracción de características:** El vector de características se obtiene al aplicar sobre los valores de la firma una transformada Wavelet. Estas transformadas son capaces de realizar un análisis en frecuencia sin pérdida de la información espacial. La principal ventaja de este método con respecto a otros es su rapidez y la capacidad de condensar la información característica en un vector de reducido tamaño (128 bytes). Para su implementación se adecuó un algoritmo ya existente en Matlab, optimizándolo y adaptándolo para satisfacer las necesidades del entorno del microcontrolador.
4. **Almacenamiento:** Al realizar un reclutamiento, es necesario almacenar el patrón obtenido para su cotejación con la muestra adquirida en posteriores etapas de verificación. Junto con él se almacena el umbral y el número de intentos restantes, valores necesarios en posteriores etapas del proceso.
5. **Comparación:** Al solicitar la verificación del usuario, es necesario comparar el patrón almacenado con el vector de características generado en el momento de la autenticación. Para esta comparación se emplea la técnica de la distancia de Hamming, debido a la simplicidad y buenos resultados que ofrece. Por tanto, esta etapa se basa en calcular la cantidad de bits en la que difieren patrón y vector de características. De este modo, cuanto mayor sea la distancia obtenida, mayor será la diferencia existente entre el patrón y el vector extraído.

6. **Toma de decisión:** Para evaluar si la muestra obtenida se corresponde con el patrón almacenado, se compara la distancia obtenida en la etapa anterior (comparación) con el umbral almacenado en la fase de reclutamiento. Si la distancia es mayor, se rechaza la autenticación del usuario y se decrementa el contador de intentos restantes. Por el contrario, si es inferior, el resultado es una verificación válida, se permite el acceso del usuario y se restaura el número de intentos restantes a su valor inicial.
   Si el número de intentos restantes alcanza el valor de cero, el sistema se bloquea. Sólo es posible desbloquearlo, si el individuo realiza un nuevo reclutamiento.

Una vez descritas todas las etapas, en el siguiente cuadro, se indican las tareas que desempeña cada uno de los elementos del sistema para cada una de las versiones implementadas.

	Funciones a realizar	
	Terminal / Ordenador	**Token**
Versión 1	Localización del iris Obtención de la firma Extracción de características	Almacenamiento ó comparación
Versión 2	Localización del iris Obtención de la firma	Extracción de características Almacenamiento ó comparación
Versión 3	Localización del iris	Obtención de la firma Extracción de características Almacenamiento ó comparación

Con esto se consiguió una implantación de la mayoría de las funcionalidades biométricas en el Token de una manera progresiva, y una vez verificada su funcionalidad en el Terminal.

Para el intercambio de información entre el PC y el microcontrolador se eligió un protocolo similar al que emplean las tarjetas inteligentes (T=0). Es un protocolo serie maestro-esclavo, donde el PC tiene siempre el control y la iniciativa del envío de comandos. Por su parte, el microcontrolador se mantiene a la espera, y sólo responde a cada comando con el envío de una palabra de estado Además del uso de códigos CRC para asegurar la correcta transmisión de la información entre los dos extremos de la conexión, se introducen temporizadores que controlen el tiempo transcurrido entre el envío de dos caracteres consecutivos y el tiempo transcurrido entre el envío del comando y la recepción de la respuesta, para evitar que el sistema se quede bloqueado a la espera de la información necesaria por alguna de las partes.

Para finalizar, mencionar los entornos de trabajo en los que se desarrollaron cada uno de los dispositivos. La implementación del Terminal se realizó en lenguaje C++ y sobre la herramienta Borland Builder5, la cual permitió crear una interfaz gráfica de manera sencilla y estructurada en la que el usuario pudiera elegir la opción que deseaba realizar (reclutamiento o verificación).

El Token empleaba como entorno de desarrollo Keil µVision3. Esta herramienta permitió programar todas las tareas del microcontrolador en lenguaje C, el cual era automáticamente traducido a lenguaje ensamblador.

Conclusiones

Este proyecto consistió en el desarrollo de un sistema de verificación biométrica basado en el reconocimiento del iris ocular del usuario mediante la integración de una cámara comercial y un dispositivo Token, con la ayuda de un Terminal (ordenador personal).

Para ello, se partió de la implementación de dicho sistema en un PC, y poco a poco se migró cada una de las etapas del proceso de identificación al microcontrolador. Esta migración se dividió en tres versiones, de manera que en cada una de ellas, las tareas a desempañar por el Token fueron incrementándose. Esto permitió el desarrollo escalonado del sistema. De hecho, cada nueva versión supuso que el Token tuviera que ejecutar una nueva etapa del proceso de identificación biométrica, y con ello aparecieran inconvenientes y problemas que era necesario resolver para lograr finalmente su integración, y que de otra forma hubiese sido muy difícil su localización o detección y posterior resolución.

A la vista de los resultados obtenidos, se puede afirmar que el parámetro más restrictivo del sistema diseñado es la memoria que debe disponer el Token para el procesamiento de la información biométrica capturada. La completa integración del sistema de verificación sobre el microcontrolador se ha dejado como futura línea de trabajo, ya que implica la construcción de una nueva plataforma de desarrollo sobre el microcontrolador, en la que se incluyeran determinados bloques de memoria externa en los cuales fuese posible almacenar la imagen capturada por la cámara para posteriormente procesarla.

Se debe mencionar que otra línea de trabajo sería el desarrollo de la comunicación entre el Token y la cámara directamente (en este caso sería una conexión tipo USB, con un protocolo propietario a nivel de aplicación), evitando así la necesidad de utilizar un ordenador personal como dispositivo Terminal.

Originalidad

En la actualidad existen diversos y muy diferentes sistemas de identificación. Sin embargo, la gran mayoría se basan en el conocimiento de contraseñas, códigos de acceso, etc., o en el hecho de simplemente poseer algún elemento como, por ejemplo, una tarjeta o algún documento acreditativo. Estos elementos son de fácil usurpación, robo o falsificación, lo cual pone en grave peligro la eficacia del sistema.

Para mejorar estos sistemas se plantea el uso de la identificación biométrica, la cual permite identificar al individuo mediante el estudio de ciertas características físicas o del propio comportamiento de la persona.

Dentro de las posibles técnicas biométricas que pueden aplicarse (reconocimiento de voz, rasgos faciales, líneas de la mano, etc.), existen algunos productos en el mercado, de muy reciente creación, que incluyen soluciones match-on-card basadas en el estudio de las huellas dactilares. Sin embargo, los resultados que ofrecen en cuanto a rendimiento son bastante limitados.

La originalidad de este trabajo radica, no sólo en el hecho de utilizar otra técnica biométrica como es la del reconocimiento del iris ocular, sino también en el hecho de crear distintas alternativas de diseño de Dispositivos de Identificación que puedan ser aplicables a diferentes entornos.

Respecto a la técnica de reconocimiento por iris, hay que comentar que las principales bondades de esta técnica se basan en el hecho de que el iris se encuentra protegido de agentes externos por la córnea (capa transparente que fluye en su parte posterior), que, además de proteger, lo mantiene visible desde el exterior. Esto permite que el patrón del iris se mantenga estable a lo largo del tiempo. Además presenta pequeñas variaciones en su tamaño tanto con cambios en la luminosidad como cuando se ve sometido a una iluminación fija, lo cual le dota de un sencillo mecanismo para la detección de "sujeto vivo". Esto hace que ofrezca gran dificultad a la hora de posibles falsificaciones, junto con la cualidad de que sus patrones no están determinados genéticamente, por lo que incluso el ojo izquierdo y el derecho de un mismo individuo son diferentes.

El objetivo inicial de este Proyecto basado en la total integración de un sistema de autenticación en un microcontrolador, permite mejoras en la seguridad. Junto a esto hay que añadir la virtud de poder integrar un sistema de este tipo en un dispositivo de pequeño tamaño, bajo consumo y que además es portátil. Las ventajas en cuanto a seguridad radican en el hecho de poseer un dispositivo capaz de procesar directamente la información biométrica del usuario que se encuentra almacenada en su interior, sin necesidad de tener que transferir ésta a ningún otro dispositivo. Esto evita que dicha información pueda ser robada o copiada por algún usuario malicioso que pudiera posteriormente intentar suplantar la identidad del usuario en cuestión.

Además es importante mencionar que para la obtención del patrón característico que identifica al usuario, era necesario conseguir que éste fuera lo más compacto posible ya que debía almacenarse en la limitada memoria del dispositivo portátil. Por este motivo, se emplea un algoritmo matemático muy eficiente, el cual es capaz de almacenar toda esta información en tan sólo 128 bytes. Este algoritmo se basa en la medida de los cruces por cero que presenta la transformada Wavelet de la firma del iris.

Resultados

A continuación se muestran los resultados obtenidos tras el desarrollo anteriormente mencionado. Estos resultados se van a ver, tanto en la ejecución de la aplicación en el ordenador, como en el microcontrolador. Estos valores permiten comparar las versiones implementadas entre sí en cuanto a tiempos de ejecución y a tamaño del código en el microcontrolador. El análisis de los tiempos de ejecución permite comparar los resultados obtenidos al realizar las mismas tareas en los diferentes elementos del sistema.

Tiempos de ejecución

Para este análisis se tomaron medidas del tiempo que tardaba en ejecutarse los principales bloques del sistema de identificación para así estudiar si realmente poseían un tiempo de proceso razonable para su implantación y posterior utilización por parte de los usuarios. El estudio se centró en los bloques de extracción de características y de cálculo de la firma, ya que se consideró que estas etapas eran las más costosas computacionalmente, y por tanto aquellas que requerían un mayor tiempo de procesamiento.

Tiempo de ejecución (mseg)			
Acción a medir	Token		Terminal
	f = 60 MHz	f = 1.3 GHz	
Cálculo de la firma	21.21	0.40	2.12
Extracción de características	35.39	0.66	3.54

Comparando los resultados obtenidos puede observarse una gran diferencia. Esto es debido a que ambos dispositivos operan a frecuencias diferentes, siendo la frecuencia de trabajo del terminal empleado para este estudio del orden de 1.3 GHz frente a los 60 MHz del Token. Sin embargo, si se analizan estos tiempos para una misma frecuencia de trabajo, es decir si se considera que el microcontrolador trabaja a la misma frecuencia que el Terminal, puede comprobarse que el Token es más eficiente. Esto se debe a que en un PC existen varios procesos activos y un sistema operativo encargado de gestionar el porcentaje de utilización de la CPU de cada uno de ellos, mientras que el microcontrolador se encuentra únicamente a disposición del sistema de autenticación.

Los tiempos de ejecución obtenidos para una autenticación entran dentro del rango admisible en un sistema de verificación, puesto que el tiempo necesario para realizarla es del orden de 10 segundos, donde la mayor parte de este tiempo se invierte en adquirir la imagen del ojo del individuo, siendo el tiempo de proceso del orden de 3 segundos.

Tamaño del código

Tras programar y compilar cada una de las versiones desarrolladas y probadas en el token, los resultados en cuanto a tamaño del código de cada una de estas versiones fueron los mostrados en la tabla siguiente:

Tamaño del código (Bytes)			
	Datos	Constantes	Código
Versión 1	1441	44	1560
Versión 2	5031	324	2640
Versión 3	7056	90312	12936

Como puede observarse, así como se esperaba, el tamaño del código aumenta a medida que se implementaban nuevas versiones, puesto que la complejidad y cantidad de tareas que debía ejecutar el Token era mayor que para la anterior versión.

Además destacar que para la versión 3, el valor de las constantes era muy elevado, debido a que fue necesario tener que almacenar toda la información de la imagen en la memoria ROM del microcontrolador para poder probar su funcionalidad. Hay que tener en cuenta que los valores obtenidos para esta versión no pueden considerarse como definitivos, puesto que debido a la falta de memoria RAM se tuvo que almacenar previamente la imagen como valores constantes.

Aún así los tamaños de código obtenidos para las dos primeras versiones son lo bastante pequeños como para permitir su almacenamiento en cualquier tipo de dispositivo portátil. En cambio, la versión 3 requeriría disponer de un sistema con mayor capacidad de almacenamiento, debido a la gran cantidad de información que debe procesarse para realizar la autenticación o el reclutamiento de los usuarios.

Aplicabilidad

El hecho de incorporar una técnica de verificación biométrica, como es el reconocimiento del iris ocular, en un dispositivo portátil y de reducido tamaño, ofrece una ventaja competitiva frente a los sistemas tradicionales que requieren que estas tareas las realice un dispositivo dedicado. El sistema descrito en este documento posee un amplio abanico de aplicaciones en el área de la banca, tales como:

- Integración del patrón biométrico en las tarjetas inteligentes que comienzan a utilizarse en los sistemas bancarios. Esto asegura que el usuario de la tarjeta no puede ser reemplazado, lo que ofrece un gran incremento en la seguridad tanto para el usuario como para la entidad. El uso de tarjetas inteligentes dificulta la duplicación de tarjetas y el uso de técnicas biométricas que reemplacen las actuales, basadas en el conocimiento de un código PIN, protegen al usuario ante robos y fraudes.
- La utilización de técnicas biométricas y dispositivos portátiles tales como tarjetas inteligentes puede utilizarse para reforzar la seguridad de las infraestructuras PKI. De esta manera puede ofrecerse una protección más eficaz a los certificados y firmas digitales que se utilizan en este tipo de estructuras.
- El sistema propuesto puede utilizarse para proteger equipos, zonas restringidas, cámaras acorazadas, etc. mediante el control de acceso que impida el paso o utilización de determinados recursos a personal no autorizado. Además puede integrarse en los sistemas de información para controlar, el número de accesos, la hora de entrada y salida, el área o nivel de seguridad al que se accede.
- Sistemas como el descrito pueden fomentar la confianza de los usuarios en transacciones bancarias a través de la web (banca on-line) y comercio electrónico (e-commerce), si estos servicios obligasen a emplear técnicas biométricas para identificarse a la hora de realizar dichas operaciones. En este caso bastaría con que el usuario conectase el dispositivo portátil (tarjeta inteligente, Token USB) en el que se encuentra almacenado su patrón biométrico al ordenador y contar con un medio de adquisición de imágenes tales como cámaras digitales, webcams, etc.