Algoritmo para analizar señales de aceleración de firmas en el aire

J. Guerra Casanova, C. Sánchez Ávila, A. de Santos Sierra, G. Bailador del Pozo, and V. Jara Vera

Centro de Domótica Integral (CeDInt-UPM) Universidad Politécnica de Madrid
Campus de Montegancedo, 28223 Pozuelo de Alarcón, Madrid
{jguerra,csa,alberto,gbailador,vjara}@cedint.upm.es

Resumen Este artículo presenta una técnica biométrica de reconocimiento de personas aplicada a entornos móviles. Un usuario se autenticará en el sistema mediante la realización de una firma en el aire con un dispositivo móvil que integre un acelerómetro. Para el análisis de las señales de aceleración de las firmas en el aire realizadas se propone un algoritmo basado en el alineamiento de secuencias genéticas, obteniéndose un resultado de EER menor del 2 % para una base de datos de 30 personas y 4 muestras de cada firma.

Key words: Biometría, firma en el aire, dispositivos móviles, reconocimiento de gestos, seguridad, acelerómetro.

1. Introducción

Hoy en día se puede acceder a aplicaciones en Internet que pueden necesitar autenticación desde la mayoría de dispositivos móviles. Mirar el saldo de una cuenta corriente, comprar un producto en una tienda online o realizar ciertas operaciones en sitios web seguros son solo algunos ejemplos de operaciones que se pueden realizar desde un móvil con acceso a Internet y donde es importante que el usuario sea quien dice ser.

En este contexto móvil, la seguridad suele dejarse en manos de contraseñas o códigos PIN que se supone que sólo el usuario sabe. Pero, tal y como se ha comentado anteriormente, esto esconde un gran riesgo ya que las contraseñas pueden ser robadas o adivinadas comprometiendo la seguridad del sistema.

La utilización de técnicas biométricas permite solucionar estos problemas. Por un lado, el usuario no puede olvidarse de su clave, puesto que él mismo es la clave. Por otro lado, si la técnica biométrica es suficientemente distintiva, ningún usuario va a poder autenticarse en el sistema como si fuera otro, manteniendo la clave del usuario original completamente segura.

En la actualidad existen varias investigaciones que tratan de unir las técnicas clásicas de biometría en escenarios móviles, aunque hoy en día su utilización no está muy extendida. Algunas de estas líneas de trabajo son las siguientes:

- Reconocimiento de iris mediante cámaras en teléfonos móviles [1], [2], [3].

- Reconocimiento facial a través de las cámaras de los teléfonos móviles [4], [5].
- Reconocimiento por voz al hablar por teléfono [6], [7].
- Reconocimiento de la persona por la forma de andar llevando un teléfono móvil que integre un acelerémetro en el bolsillo [8], [9].
- Reconocimiento del usuario legítimo del dispositivo móvil mediante dinámica de tecleo y presión de las teclas [10].

Como puede observarse a partir del listado de técnicas biométricas en dispositivos móviles en los que se está investigando, se tiende a utilizar características identificativas del usuario que puedan ser fácilmente extraíbles con sensores ya incluídos en el propio teléfono móvil, como cámaras, micrófonos, teclas o acelerómetros.

La técnica propuesta en este artículo va acorde esta línea, puesto que se propone una nueva técnica biométrica basada en la realización de la firma en el aire sujetando un teléfono móvil, donde las características de la firma son extraídas a partir de un acelerómetro ya integrado en el teléfono. Esta restricción no es problema, debido a que hoy en día, el número de teléfonos móviles con acelerómetros es muy amplio [11], incluyéndose más y más este sensor en los modelos que salen al mercado.

2. Descripción de la técnica biométrica propuesta.

Esta técnica se basa en la realización de una firma en el aire con la mano sujetando un teléfono móvil. Para ello, es necesario que el teléfono móvil integre un acelerómetro, con el que se va a extraer la información de las aceleraciones en el eje X, Y y Z de la firma en el aire del usuario. En particular, este trabajo se ha realizado con un iPhone 3G que incluye un acelerómetro que recoge las aceleraciones en los tres ejes del espacio en un rango de (-2.5g,2.5g).

La técnica biométrica de reconocimiento de firma en 3D puede considerarse como una combinación entre las técnicas habituales de comportamiento y físicas. La repetición de una firma en el aire no depende únicamente de características de comportamiento del usuario como la manera de sujetar el teléfono móvil, sino que además influyen una serie de características físicas que van a hacer que distintas personas puedan repetir un mismo gesto de manera distinta, como por ejemplo la longitud del brazo, la capacidad de girar la muñeca, el tamaño de la mano, etc. Esta técnica es similar al reconocimiento de usuarios por firma manuscrita, pero adaptada a un entorno de teléfonos móviles, con la ventaja de poder utilizarse los tres ejes del espacio, en vez de un único plano donde realizar la firma. De hecho, al no ofrecer un plano de referencia a posibles falsificadores, la imitación de la realización de una firma en el aire es más complicada.

De igual manera, esta técnica tiene aspectos comunes con las técnicas de reconocimiento de gestos, pero el enfoque es radicalmente distinto. Las técnicas de reconocimiento gestuales intentan reconocer un mismo gesto realizado por muchas personas distintas, que lo pueden hacer de manera diferente para después

realizar una acción común a todos y en respuesta a ese gesto [12]. El enfoque en la técnica biométrica es diferenciar a la persona que realiza el gesto, así pues, si dos personas realizan el mismo gesto (o firma) en el aire, el sistema ha de ser capaz de identificar que los gestos, a pesar de su parecido, son distintos, pues corresponden a dos personas diferentes.

En esta propuesta, la extracción de características se realiza directamente en el propio móvil, sin ningún dispositivo adicional. Además, se pretende que todo el proceso de autenticación se realice también dentro del teléfono, para evitar los compromisos de seguridad en las conexiones con cualquier servidor externo. De esta manera, ejecutar todos los algoritmos involucrados en el proceso dentro del propio dispositivo móvil ofrece una gran cantidad de ventajas:

- El usuario no necesita gastarse más dinero en otros dispositivos, ya que únicamente necesita su propio teléfono móvil que ya tiene.
- Las posibilidades de ataque al sistema se reducen, ya que ninguna clave ni patrón sale fuera del dispositivo, ofreciendo una solución "Match on Card" [13].
- El sistema es resistente a ataques o caídas en las comunicaciones con un posible servidor externo que realice el proceso de autenticación.
- Esta configuración permite adoptar soluciones de criptobiometría, en el que la realización de una firma pueda generar, liberar o descifrar una clave asociada al usuario que se encuentra almacenada en el móvil, y que sólo él puede utilizar para realizar acciones que necesiten estar seguras de su identidad.

El proceso de autenticación de un usuario según esta técnica biométrica puede realizarse en un dispositivo móvil gracias al incremento de potencia de los microprocesadores de los mismos, que permiten ejecutar los algoritmos involucrados en una cantidad de tiempo razonables, logrando así alcanzar también el requisito de tiempo "real".

3. Motivación de la utilización de un algoritmo de alineamiento para el análisis de señales biométricas de firmas en el aire

En un problema de autenticación a un usuario mediante la realización de su firma manuscrita, existe el inconveniente de que un usuario nunca será capaz de repetir su firma dos veces de manera 100 % exacta, por lo que la comparación de señales nunca podrá realizarse directamente mediante la aplicación de métodos de comparación directos.

Cada vez que un usuario repite su firma, realizará ciertas partes de la misma de manera más o menos rápido, más o menos pronunciada, etc. A pesar de estas pequeñas variaciones, lo intrínsico de la firma, que permanece siempre invariante y es identificativo de la persona, sigue estando.

Por esta razón, es necesario realizar un preprocesado de la señal que corrija estas pequeñas deformaciones mediante un alineamiento, que mantenga estas

características intrínsecas de la señal, corrigiendo dichas pequeñas variaciones. De esta manera, a pesar de las pequeñas variaciones en la repetición de la firma del usuario, el sistema puede identificar la autenticidad del usuario.

De la misma manera que es importante que el algoritmo de preprocesado corrija pequeñas variaciones en la repetición de la firma, es necesario que el algoritmo no corrija "demasiado" las variaciones de la firma, puesto que en ese caso usuarios que intenten imitar la firma del usuario original, podrían hacerse pasar por él, produciendo error de falsa aceptación.

Este problema es muy parecido al problema de alineamiento global de dos secuencias genéticas, ya que trata de buscar un alineamiento máximo entre las dos secuencias de la señal biométrica. Cuanto más grande sea la subsecuencia común a las dos señales biométricas, mayor será el parecido entre ellas y por tanto, es más probable que las dos firmas sean del mismo usuario. Además, la posibilidad de introducir huecos en las secuencias que se quieran alinear permite la correción automática de las pequeñas variaciones de las secuencias de señales biométricas.

Al aplicar directamente un algoritmo de comparación entre las firmas, obtendríamos unos resultados muy altos que indicarían que las firmas corresponden a distintas personas, cuando en realidad pertenecen al mismo usuario, solo que están realizadas en distintos momentos y de distintas maneras. En particular, se pueden observar las siguientes diferencias que se pueden corregir con el algoritmo de alineamiento global:

- Las señales no comienzan en el mismo momento.
- Existen picos más pronunciados que otros.
- En algún momento de la señal, las transiciones son más lentas que otras.
- Las señales no duran exactamente lo mismo.

Por otro lado, existe una gran diferencia intrínseca a las secuencias genéticas y las señales biométricas. Las primeras son discretas, con un alfabeto cerrado, mientras que las segundas son contínuas, donde cada uno de sus puntos puede tener un valor entre (-2.5, 2.5). Debido a esta razón, es posible que el valor de dos puntos de la secuencia no coincida aunque en realidad sean iguales (por ejemplo, los valores 1.2344 y 1.2343) Esta diferencia, tal y como veremos en la Sección 5 obliga a realizar una modificación en el algoritmo que extienda el mismo al caso de alfabeto abierto y continuo.

4. Algoritmos de análisis de secuencias genéticas

4.1. Algoritmo Longest Common Subsequences

Este algoritmo permite computar de manera sencilla en análisis de la similitud de dos cadenas genéticas [14]. En este algoritmo se utilizan únicamente dos operaciones: inserción y borrado. El algoritmo, como su propio nombre indica, trata de encontrar la mayor subsecuencia común a dos secuencias dadas, ya que

los puntos de dicha subsecuencia indican que no hace falta realizar ninguna operación en ese punto de las secuencias puesto que, al ser una secuencia, común coinciden [15].

Formalmente, se define una "subsecuencia común" de dos cadenas $\mathbf{v} = v_1 \dots v_n$, $\mathbf{w} = w_1 \dots w_m$ como una secuencia de posiciones en $\mathbf{v}$, tal que $1 \leq i_1 \leq \dots \leq i_k \leq n$ y una secuencia de posiciones en en $\mathbf{w}$, tal que $1 \leq j_1 \leq \dots \leq j_k \leq m$ que cumplen que los símbolos de las posiciones correspondientes en $\mathbf{v}$ y $\mathbf{w}$ coinciden, es decir, $v_{it} = w_{jt} for 1 \leq t \leq k$.

Para representar cómo funciona el algoritmo LCS se define una matriz S, que se rellenará de manera recurrente mediante técnicas de programación dinámica. Esta matriz tendrá un tamaño $n \times m$, y se construye siguiendo la Ecuación 1:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} + 0 \\ s_{i,j-1} + 0 \\ s_{i-1,j-1} + 1, \text{ if } v_i = w_j \end{cases} \quad (1)$$

El primer término de la Ecuación 1 corresponde al caso cuando v_i no está presente en la subsecuencia común más larga de v y w (borrado en v_i). El segundo término representa el caso cuando w_j no está presente (inserción de w_j), mientras que el tercer término corresponde al caso en el que tanto v_i como w_j forman parte de la LCS. Puesto que lo que se quiere encontrar es la subsecuencia máxima común, se suma uno a cada acierto, de tal manera que al finalizar el algoritmo, el elemento $s_{n,m}$ proporcionará la longitud máxima de la cadena común a las dos secuencias originales.

Para encontrar la subsecuencia común más larga a partir de la matriz S, se busca el camino que une el elemento $s_{n,m}$ con el elemento $s_{1,1}$, teniendo en cuenta que en la Ecuación 1 si el máximo se ha conseguido a partir del primer elemento, el movimiento correspondiente es $\leftarrow$, si se ha obtenido con el segundo, el movimiento es vertical $\uparrow$ y si el término mayor es el tercero ($v_i = w_j$) se realiza un movimiento en diagonal $\nwarrow$.

El alineamiento óptimo de las señales es inmediato, incluyendo un hueco ("-") en la secuencia v por cada movimiento horizontal que se haya realizado para ir de $s_{n,m}$ a $s_{1,1}$, y un hueco en la secuencia w por cada movimiento vertical.

4.2. Generalización del Algoritmo LCS como solución a cualquier problema de alineamiento global

El algoritmo LCS proporciona una puntuación bastante restrictiva, que premia con un valor de 1 los aciertos y no penaliza las inserciones o borrados. Esta puntuación se puede generalizar, extendiendo el alfabeto A de posibles k símbolos en las secuencias a un alfabeto de $k + 1$ símbolos que incluya el símbolo "-" (gap). Además, puede definirse una matriz $\delta(x, y)$ de longitud $k + 1 \times k + 1$ que proporciona el valor de la puntuación entre cada par de posibles valores del alfabeto extendido.

De esta manera, la Ecuación 2 representa cómo se rellena la matriz S en base a esta nueva puntuación:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} + \delta(v_i, -) \\ s_{i,j-1} + \delta(-, w_j) \\ s_{i-1,j-1} + \delta(v_i, w_j) \end{cases} \quad (2)$$

Además, esta ecuación puede complementarse penalizando con una constante $-\mu$ las sustituciones, con otra constante $-\sigma$ las inserciones y borrados, y recompensando los valores iguales con una constante θ. De esta manera, puede generalizarse la computación de la matriz S mediante la Ecuación 3:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} - \sigma \\ s_{i,j-1} - \sigma \\ s_{i-1,j-1} - \mu, \text{ if } v_i \neq w_j \\ s_{i-1,j-1} + \theta, \text{ if } v_i = w_j \end{cases} \quad (3)$$

En realidad, la puntuación del algoritmo LCS no es más que un caso particular de la generalización del algoritmo, tomando los valores $\sigma = 0$, $\mu = 0$, $\theta = 1$.

Mediante esta generalización, definiendo correctamente las posibles puntuaciones de la matriz δ puede resolverse cualquier problema de Alineamiento Global, puesto que la solución obtenida será aquella que ofrece una distancia mínima de edición entre las dos secuencias que se quieren alinear.

El alineamiento óptimo global es de nuevo inmediato, incluyendo un hueco (-) en la secuencia v por cada movimiento horizontal necesario para ir de $s_{n,m}$ a $s_{1,1}$ y un hueco en la secuencia w por cada movimiento vertical.

5. Algoritmo utilizado para analizar señales de aceleraciones de firmas en el aire

Para el alineamiento de señales de aceleraciones obtenidas de firmas en el aire, es necesario redefinir la Ecuación 2, incluyendo una métrica que cuantifique cuándo dos puntos sean iguales (equivalente al $v_i = w_j$ del caso discreto y diccionario cerrado). La puntuación propuesta para el análisis de señales de firmas en el aire es la definida en la Ecuación 4:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} + \delta(v_i, -) \\ s_{i,j-1} + \delta(-, w_j) \\ s_{i-1,j-1} + \Gamma(v_i, w_j, \sigma) \end{cases} \quad (4)$$

en donde:

- La introducción de un hueco en la secuencia va a ser penalizada por una constante h, denominada "gap", cuyo valor habrá que determinar. Por tanto, en este problema definimos $h = \delta(v_i, -)$ y $h = \delta(-, w_j)$.
- La función $\Gamma(v_i, w_j, \sigma)$ es una función que proporciona una métrica para cuantificar cuánto de iguales son dos puntos de las señales. Esta función devuelve un valor muy próximo a 1 cuando v_i y w_j son muy cercanas y muy

próximo a 0 cuando no se parecen. El valor de esta función se calcula según la Ecuación 5, donde σ es otra constante cuyo valor hay que determinar para el problema en cuestión.

$$\Gamma = e^{-\frac{(v_j - w_j)^2}{2\sigma^2}} \tag{5}$$

La elección de los valores de las constantes h y σ tiene que hacerse teniendo en cuenta que las señales biométricas tratadas tienen valores entre (-2.5,2.5). En la Sección 6 se tratará de optimizar este valor para una base de datos de firmas en el aire concreta.

Realizando una interpolación de cada uno de los huecos que se han generado al aplicar este algoritmo de alineamiento a un par de señales que se quieren comparar, se obtienen las señales completamente alineadas. Éstas señales serán más parecidas cuánto más representen al mismo gesto, mantiendo sus diferencias si las firmas comparadas son distintas.

Finalmente, una vez alineadas dos señales, es necesario definir una métrica que cuantifique el parecido (o diferencia) de las dos señales ya alineadas, siendo éste el módulo de comparación de las señales preprocesadas. Para ello, se ha seleccionado la métrica basada en distancia Euclidea definida en la Ecuación 6:

$$\delta_{A,B} = \sqrt{\sum_{i=0}^{2m} (a'_i - b'_i)^2} \tag{6}$$

donde $A = \{a_1, \ldots, a_m\}$ y $B = \{b_1, \ldots, b_m\}$ son las señales de aceleración originales que se procesan y $A' = \{a'_1, \ldots, a'_{2m}\}$ y $B' = \{b'_1, \ldots, b'_{2m}\}$ las señales ya alineadas e interpoladas.

Por tanto, como resultado de todo el proceso de análisis de señales, se obtendrá un valor numérico $\delta_{A,B}$ correspondiente a la medida de similaritud de las dos señales alineadas e interpoladas, en base al algoritmo que se ha explicado. Cuanto menor sea el valor de $\delta_{A,B}$, más parecidas serán las señales, y viceversa.

Este algoritmo se utilizará para obtener el parecido de las señales en cada eje. Para calcular el parecido de dos firmas en el aire completas, hay que calcular el parecido en cada eje y realizar una media entre los valores de cada uno de los tres ejes de los que se tiene información.

6. Optimización de los parámetros h y σ del algoritmo

Para optimizar los parámetros h y σ del algorítmo explicado en la Sección 5, se ha utilizado una Base de Datos de firmas formada por 30 personas que realizaron cuatro veces un gesto en el aire con un iPhone, en el que previamente se había desarrollado una aplicación para extraer las aceleraciones de las firmas en cada eje a una frecuencia de muestreo de 100 Hz.

A partir de esta base de datos, se ha definido el siguiente experimento que se repitió para distintos valores de h y σ, para obtener los valores de EER:

- Para cada firma, se toman tres de las cuatro repeticiones de la base de datos, para conformar el patrón biométrico. Estas tres repeticiones se analizan entre ellas, de dos en dos, obteniéndose los valores $\delta_{1,2}$, $\delta_{1,3}$ y $\delta_{2,3}$, correspondientes a las diferencias de las señales de enrolamiento según el algoritmo explicado. La media de los tres valores se denomina δ_T y es propia para el patrón de cada firma en el aire.
- Para cada patrón biométrico correspondiente a cada usuario, la repetición de la firma no utilizada para formar el patrón se utiliza como un intento de acceso del usuario original. El resto de firmas del resto de usuarios se utilizan como intento fraudulento de acceso.
- Cada señal de acceso se compara utilizando el algoritmo presentado en la Sección 5 con las señales del patrón biométrico correspondientes a la firma en el aire a la que se intenta imitar para acceder al sistema, obteniéndose tres valores $\delta_{A,1}$, $\delta_{A,2}$ y $\delta_{A,3}$. El valor medio de estos tres valores, δ_A es el valor, en la métrica definida, que corresponde a cuánto se parece la señal de acceso al patrón biométrico almacenado. Si el valor δ_A de una señal de acceso respecto al patrón biométrico que se está comparando es menor que el umbral, la firma será considerada válida y si no, rechazada.
- Todo lo anterior se repite para cada conjunto de tres firmas originales para cada usuario. Es decir, para cada usuario se realiza cuatro veces el experimento, uno por cada posible combinación de las cuatro firmas que se tienen en la Base de Datos, tomadas de tres en tres elementos.
- A partir de estos cálculos se calcula la Tasa de Errores de Aceptación (FAR: False Acceptance Rate) para distintos valores de un umbral. Según el valor del umbral de acceso o rechazo de un usuario, se cuentan el número de accesos que no deberían haber accedido al sistema.
- De manera similar, se calcula la Tasa de Errores de Rechazo (FRR: False Rejection Rates) como las firmas de acceso originales que son rechazados por el sistema para distintos valores del umbral de decisión.
- El punto de corte entre las dos curvas, es el Equal Error Rate (EER) que representa el punto óptimo de decisión del umbral para tener un error total mínimo.

Este experimento se ha repetido para distintos valores de h y σ, obteniendo los resultados presentados en la Tabla 1:

Observando los resultados de dicha tabla, puede comprobarse que la configuración de $h = 0{,}4$ y $\sigma = 0{,}225$ es una de las óptimas, ya que el resultado obtenido de EER es el menor de todos. Se ha seleccionado esta configuración puesto que además, en estas condiciones se cumple que $|v_j - w_j| = 0{,}3$ y $\Gamma = h$, por lo que las puntos de la correción de las señales comenzará con valores menores de 0.3.

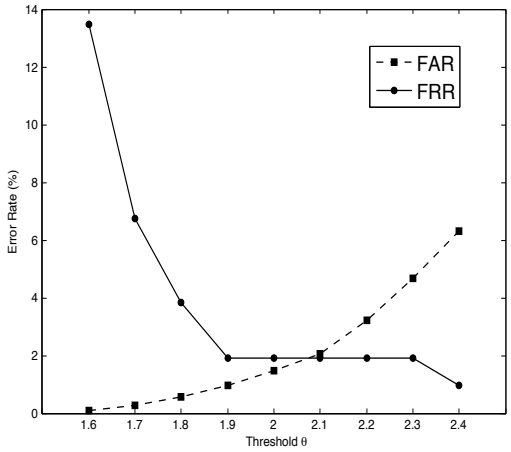
En la Figura 1 se representan las gráficas de FAR y FRR para la configuración de h y σ elegida, así como el punto de corte EER obtenido.

Los resultados de este experimento se corresponden con una prueba de falsificación "Zero-Effort", en la que los falsificadores tratan de acceder al sistema utilizando su propia firma, en vez de tratando de imitar la firma del usuario original. Un resultado de EER de 1.92 % en este tipo de prueba es muy competitivo respecto a otros trabajos similares de firma manuscrita [16], [17], [18].

Cuadro 1. Resultados de EER (%) para distintas configuraciones de h y σ.

h/σ	**0.1**	**0.15**	**0.2**	**0.25**	**0.3**	**0.35**	**0.4**	**0.45**	**0.5**
0.075	3.02	2.45	2.05	2.25	1.97	2.22	2.87	3.20	3.62
0.150	4.35	3.53	2.43	2.88	2.88	2.15	2.89	2.26	2.32
0.225	3.79	2.22	1.92	2.11	1.92	2.89	1.92	1.92	1.92
0.3	3.86	3.02	2.33	1.92	1.92	1.92	1.92	1.92	1.92

Figura 1. Tasa de error EER obtenida (%) para una configuración de $h = 0{,}4$ y $\sigma = 0{,}225$.



7. Conclusiones

En este artículo se ha presentado una técnica biométrica basada en la realización de la firma en el aire con dispositivos móviles que integren un acelerómetro, obteniéndose unos resultados prometedores para una base de datos de firmas en el aire pequeña. Estos resultados ofrecen esperanzas para seguir investigando en este ámbito, pudiéndose convertir esta técnica en una de las más utilizadas en entornos móviles en el futuro si se obtienen resultados que la validen con una base de datos de usuarios más amplia.

Referencias

1. ho Cho, D., Park, K.R., Rhee, D.W., Kim, Y., Yang, J.: Pupil and iris localization for iris recognition in mobile phones. Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, International Conference on & Self-Assembling Wireless Networks, International Workshop on **0** (2006) 197–201

2. Kurkovsky, S., Carpenter, T., MacDonald, C.: Experiments with simple iris recognition for mobile phones. Information Technology: New Generations, Third International Conference on **0** (2010) 1293–1294
3. Jeong, D.S., Park, H.A., Park, K.R., Kim, J.: Iris recognition in mobile phone based on adaptive gabor filter. In: Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006, Proceedings. (2006) 457–463
4. Tao, Q., Veldhuis, R.: Biometric authentication for a mobile personal device. Mobile and Ubiquitous Systems, Annual International Conference on **0** (2006) 1–3
5. yi Han, S., Park, H.A., Cho, D.H., Park, K.R., Lee, S.: Face recognition based on near-infrared light using mobile phone. In: Adaptive and Natural Computing Algorithms, 8th International Conference, ICANNGA 2007, Warsaw, Poland, April 11-14, 2007, Proceedings, Part II. (2007) 440–448
6. Shabeer, H.A., Suganthi, P.: Mobile phones security using biometrics. Computational Intelligence and Multimedia Applications, International Conference on **4** (2007) 270–274
7. Lapère, M., Johnson, E.: User authentication in mobile telecommunication environments using voice biometrics and smartcards. In: IS&N '97: Proceedings of the Fourth International Conference on Intelligence and Services in Networks, London, UK, Springer-Verlag (1997) 437–443
8. Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.M., Ailisto, H.A.: Identifying users of portable devices from gait pattern with accelerometers. In: Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on. Volume 2. (2005) ii/973–ii/976 Vol. 2
9. Iso, T., Yamazaki, K.: Gait analyzer based on a cell phone with a single three-axis accelerometer. In: MobileHCI '06: Proceedings of the 8th conference on Human-computer interaction with mobile devices and services, New York, NY, USA, ACM (2006) 141–144
10. Saevanee, H., Bhatarakosol, P.: User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device. Computer and Electrical Engineering, International Conference on **0** (2008) 82–86
11. Steve Dowling, Nancy Paxton, J.H.: Apple reports first quarter results. Technical report, Apple Inc. (2009)
12. Daugman, J.: Face and gesture recognition: Overview. IEEE Transactions on Pattern Analysis and Machine Intelligence **19** (1997) 675–676
13. Nilsson, J., Harris, M.: Match-on-card for java cards. Technical report, Precise Biometrics (2004)
14. Durbin, R., Eddy, S., Krogh, A., Mitchison, G.: Biological sequence analysis: Probabilistic Models of Proteins and Nucleic Acids. eleventh edn. Cambridge University Press (2006)
15. Bergroth, L., Hakonen, H., Raita, T.: A survey of longest common subsequence algorithms. String Processing and Information Retrieval, International Symposium on **0** (2000) 39
16. Nalwa, V.S.: Automatic on-line signature verification. In: Proceedings of the IEEE. (1997) 215–239
17. Jain, A.K., Griess, F.D., Connell, S.D.: On-line signature verification. Pattern Recognition **35** (2002) 2002
18. yan Yeung, D., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G.: Svc2004: First international signature verification competition. In: In Proceedings of the International Conference on Biometric Authentication (ICBA), Hong Kong, Springer (2004) 16–22