La transformada de Walsh-Hadamard y otros parámetros en la autenticación biométrica

V. Gayoso Martínez, F. Hernández Álvarez, L. Hernández Encinas, F. Montoya Vitini y A. Orúe López
Departamento de Tratamiento de la Información y Criptografía
Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)
C/ Serrano 144, 28006-Madrid, España
Emails: {victor.gayoso, fernando.hernandez, luis, fausto, amalia.orue}@iec.csic.es

***Resumen*—El patrón de iris es uno de los métodos biométricos más utilizados para la autenticación de individuos. No obstante, uno de sus principales desafíos consiste en lograr una baja tasa de falsos positivos (aceptación de un usuario ilegal) y de forma simultánea una baja tasa de falsos negativos (rechazo de un usuario legal), de modo que la seguridad del sistema sea la mayor posible. En este trabajo se presenta un primer estudio sobre la viabilidad de utilizar como método de verificación de una identidad basada en iris la transformada de Walsh-Hadamard, complementada con la covarianza cruzada y las distancias de Hamming y euclídea. Los primeros resultados muestran que la identificación basada en los cuatro parámetros anteriores presenta excelentes tasas de falsos positivos y negativos. Sin embargo, es preciso llevar a cabo estudios posteriores, que permitan ajustar mejor tales parámetros, para muestras con mayor número de usuarios.**

***Palabras clave*—Covarianza cruzada (Cross-covariance), Distancia de Hamming (Hamming distance), Distancia euclídea (Euclidean distance), Identificación biométrica (Biometric identification), Patrón de iris (Iris pattern), Transformada de Walsh-Hadamard (Walsh-Hadamard transform).**

I. Introducción

Como es sabido, la autenticación por métodos biométricos ([12], [13], [17]) consiste en verificar a individuos haciendo uso de alguno de sus rasgos fisiológicos como la cara ([6]), huella dactilar ([14]), impresión de la palma de la mano ([15]), iris ([18]), forma de la lengua ([10]), etc., o de comportamiento como la firma manuscrita ([5]), dinámica en la pulsación de teclas ([11]), olor y aroma de olor ([9]), etc.

Los sistemas biométricos ofrecen ventajas frente a otros métodos de autenticación, como los basados en contraseñas, dado que las características biométricas no se pueden perder u olvidar. Por otra parte, los rasgos biométricos son muy difíciles de copiar, falsificar, compartir o distribuir, y, además, requieren la presencia en el momento y en el lugar de quien se está identificando.

Sin embargo, a pesar de todas sus ventajas, el uso de los sistemas biométricos presenta algunos inconvenientes relacionados con la seguridad y la privacidad. Por ejemplo, algunos rasgos biométricos pueden ser grabados fácilmente sin el consentimiento del usuario, tales como la firma, voz, rostro, huella dactilar, etc. Además, a diferencia de lo que sucede con las contraseñas, PIN, etc., que se pueden renovar sin necesidad de que hayan sido comprometidos, los rasgos biométricos están asociados al usuario de forma permanente, de modo que si un rasgo se ve comprometido, no puede ser revocado o sustituido. Finalmente, si un rasgo biométrico se ve comprometido en una aplicación, todas las aplicaciones en la que este rasgo se utilice se verían comprometidas, por lo que dicho rasgo ya no será útil.

En general, el proceso para autenticar a un usuario por medio de su patrón biométrico consiste en dos fases: *inscripción* y *comprobación*. Durante la primera, se procesan por primera vez las plantillas biométricas y se almacenan en una base de datos (plantillas de referencia); mientras que en la segunda se extrae una nueva plantilla biométrica (llamada la plantilla de consulta) del usuario que quiere ser identificado y esta se compara con los datos ya almacenados (plantilla de referencia). Si la comparación es exitosa, el usuario queda autenticado; de lo contrario, su autenticación se rechaza.

El proceso de autenticación de usuarios puede llevarse a cabo de dos maneras, bien mediante una *verificación*, bien mediante una *identificación*. En el primer caso, se compara la plantilla del rasgo biométrico con la plantilla de referencia almacenada en la base de datos, es decir, el sistema realiza la comparación 1-a-1 para verificar la identidad del usuario. En la identificación, el objetivo es identificar una plantilla biométrica de un usuario desconocido como un individuo conocido dentro de un conjunto de los n posibles usuarios almacenados en una base de datos, esto es, la comparación es 1-a-n.

En general, los sistemas que utilizan un único patrón biométrico para la autenticación de individuos (unimodales) sólo disponen de la evidencia proporcionada por una única fuente de información, por lo que pueden plantear problemas relacionados con la variabilidad intra-usuarios e inter-usuarios (véase por ejemplo, [1]).

La variabilidad intra-usuarios hace referencia a las diferencias entre las plantillas de un mismo usuario extraídas en dos momentos distintos. Estas diferencias pueden causar el rechazo de un usuario legal si dos de sus plantillas son bastante diferentes (falso negativo). La variabilidad inter-usuarios se refiere a las similitudes que puede haber entre las plantillas de distintos usuarios. En este caso, tales similitudes pueden llevar a que el sistema acepte a un usuario ilegal (falso positivo).

Para paliar parte de los problemas mencionados más arriba se suelen utilizar sistemas multimodales, que utilizan varios

ISBN: 978-84-9717-323-0

patrones biométricos simultáneamente.

En todo caso, existen dos coeficientes o tasas que permiten determinar la cantidad de falsos negativos o positivos que presenta un sistema de autenticación ([16]):

- *Tasa de falsa aceptación* (False Acceptance Rate, FAR). Este coeficiente determina la probabilidad de que el sistema considere una comparación positiva entre una plantilla de consulta y una plantilla de referencia en la base de datos que realmente no coinciden, esto es, es la probabilidad de que un usuario ilegal pueda, erróneamente, ser aceptado como un usuario conocido por el sistema (falso positivo). Esta tasa mide el porcentaje de coincidencias no válidas y es una medida relacionada con la seguridad del sistema.
- *Tasa de falso rechazo* (False Rejection Rate, FRR). Este valor calcula la probabilidad de que el sistema declare, incorrectamente, la no coincidencia entre la plantilla de consulta y la plantilla de referencia en la base de datos de un mismo usuario, es decir, es la probabilidad de que un usuario legal sea rechazado por el sistema (falso negativo). Esta tasa proporciona el porcentaje de entradas válidas que son rechazadas y es un criterio de comodidad.

Asociada a esta última, está la *tasa de aceptación genuina* (Genuine Acceptance Rate, GAR). Este valor es la probabilidad complementaria de la tasa de falso rechazo, es decir, es la probabilidad de que se considere correctamente a un usuario como usuario legal (verdaderos positivos). Esto es, $GAR = 1 - FRR$.

En este trabajo se presenta un primer estudio acerca de la viabilidad de utilizar como método de verificación de una identidad basada en iris la transformada de Walsh-Hadamard, complementada con la covarianza cruzada y las distancias de Hamming y euclídea. Para determinar su eficacia se calculan la tasa de falsa aceptación y la tasa de falso rechazo haciendo uso de un determinado número de las plantillas de iris empleadas en [7], donde se ha utilizado la base de datos de iris CASIA (Chinese Academy of Sciences' Institute of Automation) ([3]).

Se ha hecho uso de los cuatro parámetros mencionados más arriba debido a que los resultados de cada parámetro son diferentes, lo que permite ajustar las tasas mencionadas de forma más precisa. Se han descartado otras métricas (simetría, identidad, máximo de coincidencia de la varianza cruzada, etc.) porque no aportan mejoras con respecto a las consideradas finalmente, bien porque sus resultados ya estaban incluidos en alguno de los parámetros considerados, bien porque no discriminaban adecuadamente. Debe tenerse en cuenta que uno de los principales objetivos es lograr que la seguridad sea máxima, es decir, que la tasa de falsos positivos sea 0.

El resto de este trabajo se organiza de la siguiente manera. En la sección II se describe el algoritmo que se propone como método de verificación, señalando las propiedades de las cuatro medidas que se han empleado para la identificación de usuarios: la transformada de Walsh-Hadamard, la covarianza cruzada y las distancias de Hamming y euclídea. La sección III contiene los resultados experimentales que se han obtenido al ejecutar el algoritmo anterior con una muestra de plantillas de irises. Finalmente, las conclusiones y trabajos futuros de esta propuesta se incluyen en la sección IV.

II. Algoritmo de verificación de plantillas de irises

Las plantillas de irises que se han considerado proceden, en concreto, de la base de datos denominada *CASIA Iris Image Database Version 1.0* ([4]) que contiene 7 ficheros BMP (Windows bitmap) de 105 ojos, lo que contabiliza un total de 735 imágenes en escala de grises de 8 bits.

El procedimiento seguido en [7] para obtener las plantillas a partir de su imagen consta de los siguientes pasos:

1. Localización del iris y la pupila.
2. Identificación de los dos conos laterales del iris, descartando los conos superior e inferior a fin de evitar distorsiones producidas por las pestañas y los párpados.
3. Normalización de los conos laterales para obtener una imagen rectangular de 1024×128 bits.
4. División de la imagen en bloques de 32×32 bits, lo que genera un total de 32×4 bloques.
5. Análisis de cada bloque mediante filtros de Gabor con 4 orientaciones $(0, \pi/4, \pi/2, 3\pi/4)$ y 3 octavos en frecuencia. Cada orientación y frecuencia, aplicadas sobre cada bloque, genera dos bits.
6. Concatenación de los $32 \cdot 4 \cdot 4 \cdot 3 \cdot 2 = 3072$ bits que dan lugar al código asociado al iris.

La Figura 1 muestra un ejemplo del procesamiento de un iris, donde junto a los sectores laterales empleados en el cálculo puede observarse la imagen rectangular normalizada correspondiente.

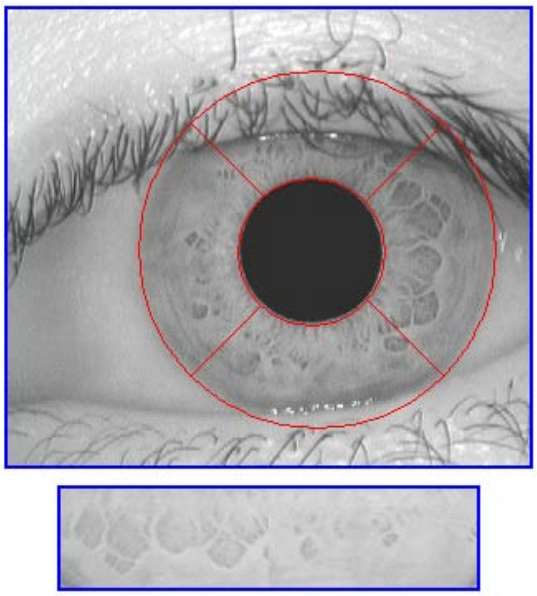

Figura 1. Ejemplo de generación de la plantilla asociada a un iris.

Los valores obtenidos se han almacenado en hexadecimal, conteniendo cada plantilla 384 bytes de información. La plantilla correspondiente a la imagen de la Figura 1 comienza de la siguiente manera:

```
9B47 CEB5 3D77 1E0C CB87 E41C 3736 9E0D
CF97 C51C 369B 8CC9 9666 665B 9A67 BA52
C466 374B 9B6D 9BD3 EC52 F74B DB6C AD92
                ...
```

En este trabajo se han programado cuatro sub-algoritmos de comparación de plantillas de iris: la distancia que proporciona la transformada de Walsh-Hadamard, la diferencia de la covarianza cruzada y las distancias de Hamming y euclídea.

Cada algoritmo suministra un valor de medida de proximidad, clasificándose el resultado como de *similitud* o *disimilitud* según que la medida arroje un resultado por encima, o por debajo, de un determinado valor de referencia elegido previamente.

La decisión de coincidencia de las plantillas de irises se toma en base a los resultados de los cuatro algoritmos de la siguiente forma: un usuario es aceptado si en alguno de los cuatro algoritmos es considerado como similar; mientras que es rechazado si es disimilar para todos ellos.

II-A. Diferencia de la Transformada de Walsh-Hadamard

La Transformada de Walsh-Hadamard (WHT) es una transformada ortogonal, similar a la transformada de Fourier, que hace corresponder a una secuencia numérica otra secuencia formada por funciones de Walsh, en lugar de funciones sinusoidales ([8]). Las funciones de Walsh solo tienen valores $+1$ y -1 y por tanto resulta la más adecuadas para transformaciones de secuencias discretas de números, mientras que la transformada de Fourier es óptima para señales continuas. La WHT es más rápida si se calcula con 512 puntos y sus resultados no mejoran calculando más puntos.

La WHT ha sido propuesta para ser empleada en la selección de características faciales ([2]). Aquí se propone su uso como un medio para la obtención de un parámetro que permita decidir si dos plantillas de irises son o no similares. A modo de ejemplo, en la Figura 2 se ilustra la WHT de la plantilla del iris del usuario 1 de la base de datos CASIA.

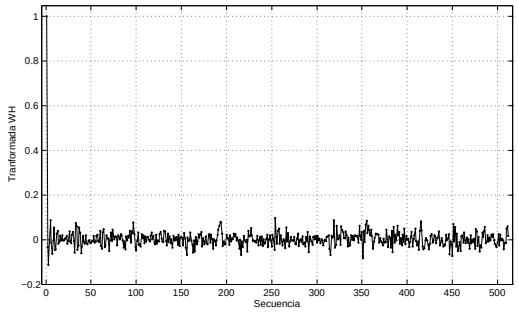

Figura 2. WHT de la plantilla del iris del usuario 1.

La Figura 3 representa la diferencia entre las transformadas de dos plantillas diferentes del iris del mismo usuario. El sub-algoritmo utilizado en este caso, consiste en calcular la diferencia cuadrática media de las secuencias de la WHT de dos irises diferentes, sean o no del mismo usuario.

La Figura 4 representa la diferencia entre las WHT de dos plantillas de irises de diferentes usuarios.

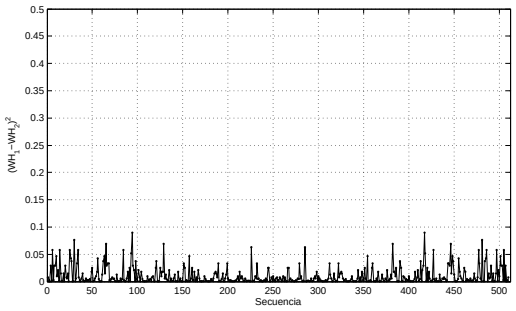

Figura 3. Diferencia entre WHT de dos plantillas del iris del usuario 1.

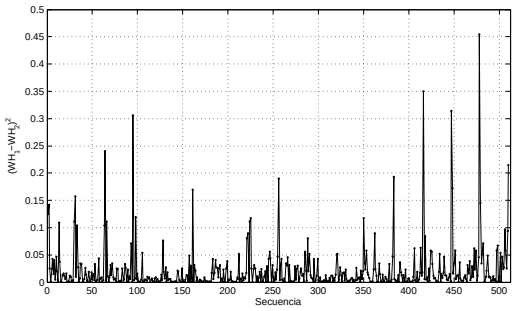

Figura 4. Diferencia entre WHT de las plantillas de los usuarios 1 y 2.

Se puede apreciar que la amplitud de la diferencia de términos de dos irises del mismo usuario es mucho menor, en conjunto, que la diferencia de términos de dos irises de distintos usuarios. Experimentalmente se ha encontrado que el valor de referencia óptimo para la diferencia cuadrática media de las secuencias de la transformada es $WH = 0{,}004$, clasificándose como *similares* los irises con valores medios menores y como *disimilares* los irises con valores mayores o iguales.

II-B. Diferencia de la covarianza cruzada

La covarianza es un valor que indica el grado de variación conjunta de dos variables aleatorias. Es el dato básico para determinar si existe una dependencia entre ambas variables. Cuando las dos variables son idénticas se denomina auto-covarianza y si son diferentes es la llamada covarianza cruzada. La Figura 5 ilustra la auto-covarianza de un patrón del iris del usuario 1 de la base de datos CASIA, normalizada para que el valor máximo sea 1.

El sub-algoritmo de comparación de irises utilizado es el siguiente:

- En primer lugar se calcula la auto-covarianza de la plantilla de un iris de determinado usuario.
- A continuación se determina la covarianza cruzada entre la misma plantilla y otra plantilla diferente (la que se desea comparar con la anterior).
- Más tarde se halla la diferencia entre ellos, término a término.
- Finalmente, se calcula la media cuadrática de estas diferencias.

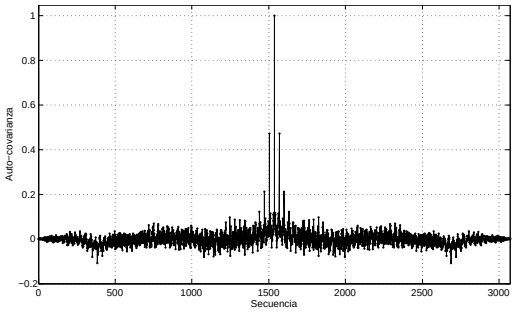

Figura 5. Auto-covarianza de la plantilla del usuario 1.

La Figura 6 ilustra la covarianza cruzada entre dos plantillas diferentes del iris del usuario 1 de la base de datos CASIA. La Figura 7 ilustra la covarianza cruzada de una de las plantillas de iris del usuario 1 y otra del usuario 2. Se puede apreciar que la covarianza cruzada de dos irises del mismo usuario es mucho menor, en conjunto, que la covarianza cruzada de patrones de dos irises de distintos usuarios.

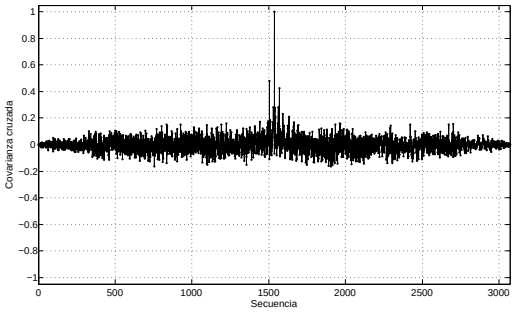

Figura 6. Covarianza cruzada de dos plantillas del usuario 1.

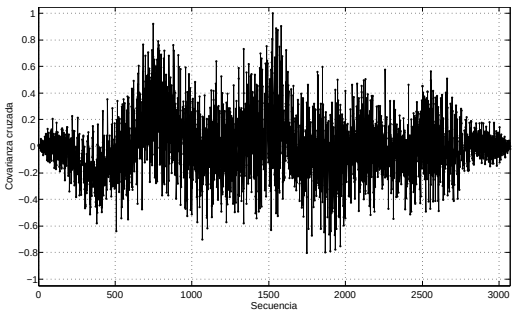

Figura 7. Covarianza cruzada de las plantillas de los usuarios 1 y 2.

Experimentalmente se ha encontrado que, dados los valores de prueba considerados, el valor de referencia óptimo para la diferencia cuadrática media de las covarianzas cruzadas de las secuencias de la transformada es $Xv = 0{,}01$, clasificándose como *similares* los irises con valor de esta diferencia menor que el valor de referencia y como *disimilares* los irises con valores mayores o iguales.

II-C. Distancia de Hamming

Para comparar dos archivos de plantillas de irises de la misma longitud de m muestras, se determina el valor medio de las distancias de Hamming entre las muestras que ocupan el mismo lugar en cada archivo.

La distancia de Hamming dh se ha determinado contando la cantidad de bits idénticos en ambas muestras. Se han utilizado muestras codificadas con 2 bits, por lo que esta distancia puede ser 0, 1 o 2. Experimentalmente se ha encontrado que un valor de referencia con buenos resultados es $DH = 0{,}5$. Así, se clasifican como *similares* las plantillas de irises cuyo valor medio de distancias de Hamming son menores que dicho valor, $dh < DH$, y como *disimilares* las plantillas con valores iguales o mayores que el dado, $dh \geq DH$.

II-D. Distancia de euclídea

Consiste en un sub-algoritmo similar al anterior, que en lugar de calcular la distancia de Hamming entre las muestras de las plantillas de irises calcula la media de la diferencia euclídea de los valores absolutos de las muestras de los patrones, que puede variar, en decimal, entre 0 y 3.

Experimentalmente se ha encontrado que el valor de referencia óptimo es $DE = 1$, clasificándose como *similares* los iris con valor medio de distancias euclídeas menores que este valor y como *disimilares* los iris con valores iguales o mayores que el de referencia.

III. Resultados experimentales

En la parte experimental se han considerado las plantillas de los 7 irises de 105 individuos de la base de datos CASIA ([3]). Estas 735 plantillas han servido como base de datos para contrastar el rendimiento del algoritmo presentado en la sección II.

Dado que se trata de analizar los valores de las tasas de falsa aceptación (*FAR*) y falso rechazo (*FRR*), se ha ejecutado el algoritmo presentado en la sección II de modo que cada una de las 7 plantillas de irises de cada uno de los 105 usuarios se ha comparado con las $735\ (= 105 \cdot 7)$ plantillas de la base de datos, obteniéndose una tabla de tamaño 735×735 (se omite la presentación de esta tabla por razones de espacio).

Para el estudio de la variabilidad intra-usuarios, cada una de las 7 plantillas de los 105 usuarios se considera como la entrada de la fase de verificación y se compara con el resto de las plantillas del mismo usuario. El resultado de esta comparación muestra el nivel de similitud entre todas las plantillas de un único usuario. El número de similitudes permite medir la tasa de falso rechazo. Así pues, si se consideran todas las comparaciones de un usuario consigo mismo se obtienen $49\ (= 7 \cdot 7)$ comparaciones, de modo que el número total de comparaciones es de $5145\ (= 49 \cdot 105)$. En el experimento realizado se ha obtenido que las comparaciones exitosas entre los 105 usuarios es el siguiente valor:

$$\mathit{GAR} = \frac{4091}{5145} \approx 0{,}7951 \equiv 79{,}51\,\%.$$

Por tanto, se tiene que la tasa de falso rechazo, es decir, los falsos negativos son:

$$FRR = 1 - GAR \approx 1 - 0{,}7951 = 0{,}2049 \equiv 20{,}49\,\%.$$

Considerando cada uno de los parámetros por separado, los resultados que se han obtenido son los siguientes: la distancia euclídea proporciona un $65{,}34\,\%$ de verdaderos positivos, la distancia de Hamming un $71{,}21\,\%$, la covarianza cruzada un $71{,}43\,\%$ y la WHT un $69{,}05\,\%$; mientras que considerando todas juntas, el resultado es del $79{,}51\,\%$, lo que supone una ganancia considerable. Además, ninguno de los parámetros proporciona falsos positivos.

Como era de esperar, la aportación a la verificación de cada uno de los parámetros es diferente. Así, si no se considera alguno de los parámetros, la tasa de verdaderos positivos disminuye, especialmente si no se considera la distancia de WHT, en cuyo caso los verdaderos positivos serían solamente del $76{,}95\,\%$. Por tanto, es necesario incluir esta transformada entre los parámetros de discriminación para obtener mejores resultados, aunque su coste computacional sea el más elevado.

En el estudio de la variabilidad inter-usuarios, se compara cada una de las 7 plantillas de cada uno de los 105 usuarios con las 7 plantillas de los restantes 104 usuarios y se determina su similitud o disimilitud. Dado que hay un total de 535080 $(= 7 \cdot 105 \cdot 7 \cdot 104)$ comparaciones y no hay disimilitudes, la tasa de falsa aceptación, es decir, los falsos positivos son:

$$FAR = \frac{0}{535080} = 0{,}0 \equiv 0\,\%.$$

Finalmente, el coste computacional, para comparación, del algoritmo de la distancia euclídea es de $0{,}19$ ms, de la distancia de Hamming es $0{,}55$ ms, de la varianza cruzada es $0{,}87$ ms y de la WHT es $5{,}22$ ms. La comparación de una plantilla contra las 735 de la base de datos requiere $4{,}7$ segundos. Debe tenerse en cuenta que los algoritmos se han ejecutado bajo MatLab en un PC de 2 GHz, por lo que sería posible obtener mejores resultados si estos se implementaran en C, por ejemplo.

IV. Conclusiones

Con el fin de mejorar las tasas de falsos positivos y falsos negativos en la identificación de usuarios mediante plantillas de irises, se ha propuesto el uso de un algoritmo que considere cuatro parámetros derivados de las distancias de la transformada de Walsh-Hadamard y de la covarianza cruzada, así como de las distancias de Hamming y euclídea.

Este algoritmo considera que dos plantillas de irises son similares, y por tanto que ambas pertenecen a un mismo individuo, si alguno de los cuatro parámetros anteriores declaran ambas plantillas como similares. En caso contrario, esto es, si ninguno de los cuatro parámetros lo considera similar, las plantillas se consideran disimilares y la identificación es rechazada.

El algoritmo, en su versión actual, permite utilizar una única fuente de información (unimodal), proporcionando una tasa de falsos negativos del $20{,}49\,\%$ y de faltos positivos del $0\,\%$. Esto es, según el algoritmo propuesto y con la muestra de usuarios empleada, no se aceptan individuos ilegales ($FAR = 0{,}0$) a la vez que el porcentaje de individuos legales que son erróneamente rechazados es cercano al $20\,\%$ ($FRR = 0{,}2049$).

A la vista de los resultados obtenidos, es necesario incluir la transformada de Walsh-Hadamard entre los parámetros del algoritmo para mejorar los resultados, aunque su coste computación sea el más elevado.

Agradecimientos

Este trabajo ha sido parcialmente subvencionado por el Ministerio de Ciencia e Innovación (España) bajo el proyecto TIN2011-22668.

Referencias

[1] R. Alvarez Marino, F. Hernandez Alvarez, and L. Hernandez Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," *Information Sciences*, vol. 195, pp. 91–102, 2012, http://dx.doi.org/10.1016/j.ins.2012.01.042.

[2] W. Besbas, M. Artemi, R. Sullivan, and M. Al Rjebi, "Content based face image retrieval in Walsh Hadamard transform domain," in *The International Conference on Computing, Networking and Digital Technologies (ICCNDT2012)*, 2012, pp. 101–106.

[3] Biometric Ideal Test, "CASIA iris image database," 2010, http://biometrics.idealtest.org/findDownloadDbByMode.do?mode=Iris.

[4] ——, "CASIA iris image database, version 1.0," 2010, http://www.idealtest.org/dbDetailForUser.do?id=1.

[5] R. Blanco-Gonzalo, O. Miguel-Hurtado, A. Mendaza-Ormaza, and R. Sanchez-Reillo, "Handwritten signature recognition in mobile scenarios: Performance evaluation," in *2012 IEEE International Carnahan Conference on Security Technology (ICCST'2012)*, 2012, pp. 174–179.

[6] J. Connolly, E. Granger, and R. Sabourin, "An adaptive classification system for video-based face recognition," *Information Sciences*, vol. 192, no. 1, pp. 50–70., 2012.

[7] E. Diez Laiz and C. Sanchez Avila, "Sistema criptobiométrico basado en iris para esquemas Diffie-Hellman con curva elíptica (ECDH)," in *Congreso de Métodos Numéricos en Ingeniería*, 2009, pp. 1–20.

[8] D. Elliot and K. Rao, *Fast transforms, algorithms, analysis, applications*. New York: Academic Press, 1982.

[9] V. Fernandez Mateos, F. Hernandez Alvarez, L. Hernandez Encinas, C. Sanchez Avila, and G. Bailador, "Towards a biometric identification based on corporal odor," in 4^{th} *International Information Security & Cryptology Conference (ISCTURKEY'10)*, May 2010.

[10] B. Huang, J. Wu, Z. Zhang, and N. Li, "Tongue shape classification by geometric features," *Information Sciences*, vol. 180, pp. 312–324, 2010.

[11] J. Ilonen, "Keystroke dynamics," 2013, http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf.

[12] A. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. New York: Springer, 1999.

[13] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.

[14] A. Jain, A. Ross, and S. Prabhakar, "Fingerprint matching using minutiae and texture features," in *International Conference on Image Processing (ICIP)*, 2001, pp. 282–285.

[15] H. Li, J. Zhang, and Z. Zhang, "Generating cancelable palmprint templates via coupled nonlinear dynamic filters and multiple orientation palmcodes," *Information Sciences*, vol. 180, pp. 3876–3893, 2010.

[16] J. Mainguet, "Biometrics," 2013, http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm.

[17] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer, 2003.

[18] C. Sanchez Avila and R. Sanchez-Reillo, "Two different approaches for iris recognition using Gabor filters and multiscale zero-crossing representation," *Pattern Recognition*, vol. 38, no. 2, pp. 231–240, 2005.