Revista Cubana de Ciencias Informáticas
Vol. 9, No. 4, Mes Octubre-Diciembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 132-141

Tipo de artículo: Artículo original
Temática: Reconocimiento de patrones
Recibido: 20/07/2015 | Aceptado: 02/10/2015

Extracción de características identificativas en plantillas de minucias mediante la estructura compleja

Method for minutiae representation and identifying information extraction on fingerprint templates

Ramón Santana Fernández[1*], **Adrián A. Machado Cento**[1], **Vivian Estrada Sentí**[1]

[1]Universidad de las Ciencias Informáticas, carretera San Antonio de los Baños km $2\frac{1}{2}$, Reparto. Torrens, Boyeros, La Habana. Cuba. CP.: 19370 rsfernandez@uci.cu

[*]Autor para correspondencia: rsfernandez@uci.cu

Resumen
La identificación de personas mediante rasgos biométricos, como la huella dactilar, es considerada un mecanismo de autenticación segura. Los sistemas criptográficos propuestos para la protección de plantillas de minucias de huellas dactilares necesitan realizar el proceso de alineación de las plantillas biométricas debido a la variabilidad que presentan los datos en diferentes muestras del mismo rasgo. Los modelos de alineación propuestos en la bibliografía basan su funcionamiento en la selección de un punto focal, la formación de estructuras de minucias o la detección de las singularidades de la huella dactilar. Estas características pueden estar o no presentes en la huella dactilar, pueden variar de una muestra a otra y pueden ser seleccionadas de manera errónea, lo que ocasiona una pérdida del rendimiento de sistema de autenticación. La presente investigación tiene como objetivo la formulación de un método de representación de la información contenida en las plantillas de minucias y la extracción de características identificativas, invariantes a rotación y traslación, que posibilite el análisis de las características obtenidas de las minucias de manera local y global, para disminuir el impacto de la eliminación de minucias reales y la inclusión de minucias falsas, utilizando la combinación de dos estructuras de minucias. El proceso está compuesto por 3 etapas: formación de la estructura compleja de minucias, extracción de características invariantes a rotación y traslación provenientes de las tripletas y la clasificación de las características extraídas. El proceso de comparación se realiza mediante el cálculo de similitud existente entre cada estructura compleja.

Palabras claves: Bio-criptografía, alineación, plantillas de minucias, protección biométrica, estructuras de minucias

Abstract
Identifying people using biometric features such as fingerprints, it is considered a secure authentication mechanism. Cryptographic systems proposed for the protection template fingerprint minutiae need to perform the alignment process of the biometric templates due to variability of data in different samples of the same feature. Alignment models proposed in the literature base their operation on the selection of a focal point, the formation of structures of minutiae or detection of the singularities of the fingerprint. These features may or may not be present in the fingerprint, they may vary from one sample to another and may be selected wrongly, consequently resulting in loss of performance of authentication system. This research aims at developing a method of representing the information contained in the minutiae templates and identifying characteristics extraction,

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 4, Mes Octubre-Diciembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 132-141

rotation and translation invariant, which enables the analysis of the characteristics of the minutiae obtained locally and overall, to lessen the impact of the elimination of real minutiae and the inclusion of false minutiae, using the combination of two structures minutiae. The process consists of 3 stages: formation of the complex structure of minutiae extraction invariant to rotation and translation characteristics from triplets and classification of the extracted features. The comparison process is performed by calculating similarity between each complex structure.

Keywords: *minutiae structure, information representation, minutiae template, template protection.*

Introducción

La utilización de sistemas biométricos para la identificación de personas en tareas diarias tales como transacciones bancarias, controles de acceso o en la telefonía móvil ha despertado un creciente interés en la integridad y confidencialidad de los datos transmitidos. La utilización de redes públicas con menor grado de seguridad que las redes privadas aumenta la posibilidad de obtención de los datos biométricos mediante diferentes tipos de ataques informáticos, especialmente si los datos son transmitidos en texto plano. Como consecuencia la privacidad y seguridad de los datos biométricos se ve comprometida, lo que constituye uno de los problemas (DAHIYA and KANT, 2012) más preocupantes y difíciles en la actualidad en este campo de estudio.

La huella dactilar, como identificador biométrico, presenta un conjunto de variaciones (rotación, translación, superposición parcial y deformación no lineal) descritas en (JAIN et al., 2013; MALTONI et al., 2009), las cuales dificultan el proceso de comparación en el dominio cifrado. Como alternativa de solución y para aumentar el número de minucias coincidentes, se plantea alinear los datos cifrados con los datos a comparar antes de realizar el proceso de comparación en el dominio protegido. Para el alineamiento de plantillas de minucias han sido propuestos varios enfoques (JEFFERS and ARAKALA, 2007; JAIN et al., 2013) destacando en cada uno de ellos sus fortalezas y debilidades. Entre los enfoques más citados en la bibliografía se encuentran la obtención de una minucia de referencia o punto focal (BOONCHAISEREE and AREEKUL, 2009), la detección de las singularidades núcleo y delta (MALTONI et al., 2009), la formación de estructuras de minucias (JEFFERS and ARAKALA, 2006) y el cálculo de los puntos de mayor curvatura (ZHANG et al., 2014). Estos métodos de alineamiento presentan varios inconvenientes ampliamente descritos en la bibliografía entre los que se encuentran la selección errónea del punto focal o la minucia de referencia, la ausencia de los puntos singulares en las huellas dactilares pertenecientes a la clase arco, así como la posibilidad de aparición o no de estas características en alguna toma. Se analiza además la ausencia, cambio o introducción de minucias falsas en la formación de estructuras triangulares. Como principal consecuencia de estas dificultades está la afectación del rendimiento del sistema biométrico en términos de tasas de falsos aceptados y falsos rechazos. Otro de los inconvenientes es el relacionado con el cálculo de los puntos de máxima curvatura, el cuál es un algoritmo iterativo, ocasionando serias dificultades en el rendimiento del sistema en términos de costo computacional y

tiempo de respuesta.

Otro enfoque predominante en los últimos años como se puede apreciar en (LI et al., 2008; ZHE and JIN, 2011; ZHANG et al., 2014) es la formulación de modelos de protección de plantillas de minucias invariantes a rotación y traslación, basados en información identificativa obtenida a partir de las estructuras de minucias. En este enfoque se transforma la información proveniente de las minucias de coordenadas (x, y) y ángulo a otra forma de representación al extraer un conjunto de características identificativas específicas de cada estructura para ser aseguradas utilizando los métodos de cifrados bóveda difusa (JUELS and SUDAN, 2006), plantillas cancelables (RATHA et al., 2007) o biohashing (JIN et al., 2004; BELGUECHIL et al., 2010). Este proceso de manera general es realizado a partir de la creación de un conjunto de estructuras de minucias. De las estructuras formadas se extrae un conjunto de características identificativas, invariantes a rotación y traslación y resistentes a la deformación no lineal, que son cifradas utilizando los métodos planteados.

En (JEFFERS and ARAKALA, 2006) se analizan las tripletas de minucias, las 5 vecindades locales y el diagrama de Voronoi como formas de representación de las plantillas de minucias y su factibilidad para ser utilizadas en el proceso de alineamiento, con el objetivo de conocer cuáles de estas son invariantes a rotación y traslación y cuáles presentan el mejor rendimiento en su creación. Como resultado se obtiene que las tripletas de minucias y el diagrama de Voronoi son invariantes a rotación y traslación. En (ZHE and JIN, 2011) se describe un modelo de protección de plantillas de minucias utilizando las n vecindades de una minucia y las tripletas que se pueden formar en ella, con n = 3. En (JEFFERS and ARAKALA, 2007) se realiza un estudio de estas estructuras con el objetivo de obtener la que mejor rendimiento tiene para alinear los datos para ser utilizados en el esquema bóveda difusa, utilizándose como dato de ayuda en el proceso de alineación las coordenadas del núcleo, las cuales pueden aparecer o no en diferentes tomas de huellas dactilares. Los trabajos (LI et al., 2008; GHANY et al., 2012) explican diferentes enfoques para la protección de plantillas de minucias de huellas dactilares con información, invariante a rotación y traslación, obtenida de las minucias.

En todos los casos existen limitaciones que afectan negativamente el rendimiento del proceso de comparación de plantillas protegidas. En el caso de los trabajos propuestos en (ZHE and JIN, 2011; AHMAD, 2013; WANG and HU, 2014) se ven afectado por la eliminación de minucias reales o la introducción de falsas minucias. La nueva información añadida impacta negativamente en el proceso de comparación debido al enfoque global en el análisis de las características obtenidas de las minucias. En todos los casos se realiza la obtención local de la información referente a las minucias, sin embargo el análisis para realizar el proceso de comparación se realiza de manera global. Los cambios en la información identificativa afectan negativamente este proceso al ser evaluados solo de manera global. La principal razón se debe a que la comparación local permite calcular un índice de similitud local que puede ser evaluado de manera global para descartar estructuras donde la información no es acertada. En (ULUDAG et al., 2005) se asume que el proceso de alineación ha sido realizado manualmente

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 4, Mes Octubre-Diciembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 132-141

durante la ejecución de las pruebas, hecho que no es consistente con un sistema de reconocimiento mediante huellas dactilares en ambientes reales. La presente investigación tiene como objetivo principal la formulación de un método de representación de la información contenida en las plantillas de minucias y extracción de características identificativas a partir de este, que posibilite el análisis de las características obtenidas de las minucias de manera local, para disminuir el impacto de la eliminación de minucias reales y la inclusión de minucias falsas, utilizando la combinación de dos estructuras de minucias.

Materiales y métodos o Metodología computacional

La formulación de modelos de protección de plantillas de minucias de huellas dactilares que no realizan el proceso de alineación realizan el cifrado a partir de un conjunto de datos extraídos de las minucias. Para la representación de la información contenida en las plantillas de minucias y la extracción de datos invariantes a rotación y traslación varios modelos han sido propuestos en la bibliografía. Entre ellos se encuentran un conjunto de estructuras topológicas (JEFFERS and ARAKALA, 2006) para obtener las características identificativas provenientes de las minucias y realizar el proceso de cifrado con diferentes métodos.

En (AHN et al., 2008) se describe un modelo de representación y extracción de características identificativas provenientes de las minucias, invariantes a rotación, traslación y deformación no lineal las cuales serán cifradas. El proceso de extracción comienza con la selección de tres minucias de la plantilla de minucias, a continuación se forma un círculo donde las minucias se encuentran en el borde, se calcula el circuncentro de la tripleta y los ángulos formados entre cada vértice del triángulo y el circuncentro. Para realizar el cifrado se almacenan como características identificaticas: las coordenadas del circuncentro $(x'; y')$, se selecciona el ángulo mayor ϕ_{12} y su vecino o ángulo adyacente ϕ_{23} siguiendo la dirección de las manecillas del reloj, los ángulos $\sigma_1, \sigma_2, \sigma_3$ y el tipo δ como se muestra en la figura 1.

En (XI and HU, 2009) se propone una característica compuesta, invariante a rotación y traslación para obtener un conjunto de características identificativas y realizar el cifrado con una variante del modelo de bóveda difusa. Este modelo es propuesto para utilizarse en la verificación de identidad en dispositivos móviles. La característica propuesta se define como la relación entre dos minucias expresadas por la longitud de la recta que las separa, la diferencia de orientación de los ángulos de cada minucia y el ángulo formado por rectas paralelas a la dirección de las minucias. Las relaciones se determinan utilizando estructuras de n vecindades más cercanas, siendo $n = 4$. Se forma un vector de 4 dimensiones, invariante a rotación y traslación que es cifrado con el modelo de bóveda difusa y comparada por el algoritmo Comprobación de estructura jerárquica (HSC) propuesto.

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 4, Mes Octubre-Diciembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 132-141

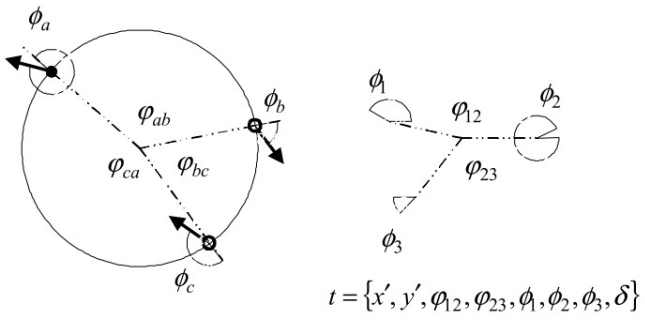

Figura 1. Características identificativas extraídas a partir de tres minucias minucias

Método propuesto

El método que se propone en la presente investigación se describe, de manera general, como se muestra a continuación. El proceso de extracción de características identificativas provenientes de las minucias está compuesto por 3 etapas:

1. Formación de la estructura compleja de minucias.
   - *a*) Formación de la estructura 5 vecindades más cercanas a una minucia.
   - *b*) Extracción de las tripletas que pueden formarse utilizando el centro y las minucias vecinas de la estructura.
2. Extracción de características invariantes a rotación y traslación provenientes de las tripletas.
3. Clasificación de las características extraídas.

La estructura compleja está conformada por la unión de dos estructuras de minucias, las 5 vecindades más cercanas y las tripletas de minucias propuestas en (JEFFERS and ARAKALA, 2006). Inicialmente se realiza la selección de un punto central $A(x, y)$ dentro del conjunto de minucias $Z(x, y, \alpha, t)$ donde x, y representan las coordenadas en el espacio cartesiano, α representa el ángulo y t el tipo de minucia partir de la ecuación 1.

$$\sum_{i=1}^{n} \frac{x_i}{n}; \sum_{i=1}^{n} \frac{y_i}{n}; \tag{1}$$

La selección de este punto permite establecer un orden en la creación de las estructuras de minucias y tiene como objetivo simplificar el proceso de comparación. Partiendo del punto $A(x, y)$ se seleccionan las minucias

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 4, Mes Octubre-Diciembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 132-141

$Z_i(x, y)$ más cercanas a él utilizando la función de distancia $\lambda = min(z_{i \in E})\ d(A, Zi)$ dónde i toma valores de 0 a 5 y d es representado como la distancia euclidiana entre dos puntos. Se propone realizar la selección de 5 minucias más cercanas debido a que experimentos realizados por el autor demuestran que el índice de afectación de una estructura, al incluir o eliminar una minucia que no estaba en la colección original, es significativamente menor que utilizando 3 minucias como se propone en (ZHE and JIN, 2011).

La estructura formada contiene 6 minucias, una minucia central y 5 vecindades. Esta estructura es descompuesta en un conjunto de tripletas de minucias que son formadas a partir de las relaciones entre ellas. A cada tripleta se le adiciona un descriptor denominado tripleta primaria o secundaria:

1. Primaria: Cuando uno de sus vértices coincide con la minucia central.
2. Secundaria: Cuando ninguno de sus vértices coinciden con la minucia central.

De esta manera es posible medir la fortaleza de las conexiones entre cada una de las minucias que conforman una tripleta mediante su conexión con la minucia central y con las demás minucias que forman parte de la estructura. De cada tripleta se extrae un conjunto de características identificativas para formar un vector de la manera $S_1, S_2, S_3; \alpha_1, \alpha_2, \alpha_3; \Delta\sigma_1, \Delta\sigma_2, \Delta\sigma_3$. La longitud de los lados se representa como S_1, S_2, S_3, los ángulos internos son representados como $\alpha_1, \alpha_2, \alpha_3$ y la diferencia de los ángulos de las minucias adyacentes a un lado representada como $\Delta\sigma_1, \Delta\sigma_2, \Delta\sigma_3$ se calcula mediante la expresión $\Delta\sigma_1 = dif(anguloc_{i2}, anguloc_{i1})$ como se muestra en la figura 2.

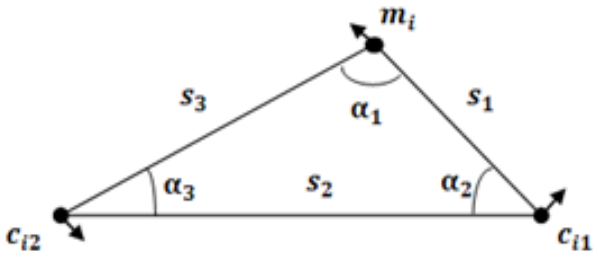

Figura 2. Características identificativas extraídas de las tripletas de minucias

La clasificación de los datos obtenidos es un proceso mediante el cual, en dependencia del descriptor asociado a las tripletas, los vectores resultantes son clasificados en primarios o secundarios. El proceso de comparación se realiza mediante el cálculo de similitud S que existe entre cada estructura compleja. Para ello se realiza

Revista Cubana de Ciencias Informáticas
Vol. 9, No. 4, Mes Octubre-Diciembre, 2015
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 132-141

una comparación cruzada donde para cada $d_{(i,j)}, i = 1...n$ y $j = 1...n$ dónde $n$es el número de estructuras en cada conjunto y $d_{(i,j)}$ representa la comparación entre dos estructuras. El cálculo de S se realiza mediante la fórmula 2:

$$S = \frac{tp(d_{(i,j)})}{100} + \frac{ts(d_{(i,j)})}{100} \tag{2}$$

tp representa los datos pertenecientes a las tripletas primarias y ts los datos pertenecientes a las tripletas secundarias. La comparación de cada tripleta de minucias se realiza según el índice de similitud que presentan los datos en comparación con un umbral definido. En el caso de los lados se define el descriptor desfasamiento, el cual es la diferencia en pixeles de la longitud de un lado con respecto al otro. En el caso de los ángulos internos y la diferencia de los ángulos de minucias adyacentes a un lados, se define el descriptor grados de libertad como la diferencia existente entre dos ángulos a comparar. Ambos descriptores actúan como umbrales para calcular el índice de similitud entre dos estructuras. El método propuesto en la presente investigación elimina la necesidad de realizar el proceso de alineación debido a la selección de estructuras invariantes a rotación y traslación. La creación de la estructura compleja mejora la tolerancia a cambios en los conjuntos de minucias de prueba y de muestra. La eliminación o reemplazo de una minucia en el conjunto de prueba con respecto al conjunto de muestra afecta en menor medida que lo propuesto en (ZHE and JIN, 2011) debido a que la cantidad de información que es utilizada en el método propuesto es mayor.

Resultados y discusión

El rendimiento del método propuesto se analiza teniendo en cuenta dos aspectos fundamentales, los índices de similitud entre dos estructuras coincidentes y entre dos estructuras no coincidentes y las tasas de falsos aceptados y falsos rechazos calculadas. Para la obtención de las plantillas de minucias se utilizó un SDK proveído por la empresa Innovatrics y se analizaron las bases de datos FVC2000 DB1-B y DB2-B. Cada base de datos está compuesta por imágenes de huellas dactilares pertenecientes a los 10 dedos de la mano, con 8 impresiones por dedo, para un total de 80 imágenes. Las imágenes están etiquetadas como 101_1 donde, 101 es el identificador del dedo al cual pertenece la imagen y 1 es el número de la muestra. En el proceso de comparación se fijaron los parámetros: grados de libertad $(GL) = 10°$, y el desfasamiento entre lados $(DL) = 5px$. Se eliminaron del proceso de comparación las tripletas cuya suma de dos lados fuese mayor que 150° debido a que se observó poca formación de este tipo de tripletas en dos tomas diferentes del mismo rasgo. La medición del primer aspecto se realizó mediante el cálculo del porciento de tripletas primarias y secundarias coincidentes entre la plantilla de muestra y la plantilla candidata. Este es denominado índice de similitud y se utiliza como umbral para el cálculo de las tasas de falso aceptado y falso rechazo. En la tabla 1 se muestran

los valores límites debido a la cantidad de datos obtenidos. La medición de las tasas de falsos aceptados y falsos rechazos se calcularon teniendo en cuenta el umbral de similitud total calculado a partir de los índices de similitud de las estructuras complejas. Se selecciona este umbral basado en la idea de igualar las tasas de falsos aceptados y falsos rechazos.

Tabla 1. los resultados límites del índice de coincidencia para estructuras que coinciden (TM) y para las que no coinciden (TNM).

Bases de datos	**Mayor índice TM**	**Menor índice TM**	**Mayor índice TNM**	**Menor índice TNM**
DB1-B	51.63	1.24	7.08	0
DB2-B	49.69	1.00	6.46	0

Tabla 2. Se representan las tasas de falso aceptado, falso rechazo (FMR y FRR) y el índice de similitud umbral (ISU)

Base de datos	**FMR**	**FRR**	**ISU**
DB1-B	0.021519	0.0278481	3.30
DB2-B	0.020886	0.0218354	3.30

para la comparación de plantillas de minucias de huellas dactilares. La clasificación de las tripletas de minucias que componen la estructura aumenta el nivel de discriminación de los datos, lo que mejora el rendimiento del proceso de comparación. Los índices de similitud obtenidos a partir de la comparación de las estructuras están condicionados a la cantidad de minucias y de estructuras que pueden formarse. A mayor cantidad de minucias en la plantilla a analizar mejor índice de similitud es obtenido. Las tasas de error calculadas muestran la factibilidad de realizar la comparación de estas estructuras.

Conclusiones

El método propuesto permite disminuir el impacto de la eliminación de minucias reales y la inclusión de minucias falsas, utilizando la combinación de dos estructuras de minucias. La obtención de 5 vecindades más cercanas a una minucia y la formación de tripletas de minucias a partir de estas brindan un conjunto de datos identificativos para la comparación de plantillas de minucias que brindan información más precisa sobre un segmento de la huella dactilar invariante a rotación y traslación y resistente a adición o eliminación de minucias. La clasificación de las estructuras en primarias y secundarias permite la evaluación local y global de los datos durante el proceso de comparación. La creación de tripletas de minucias a partir de las 5 vecindades de una minucia y el análisis global y local de los datos obtenidos disminuye el impacto de variaciones en la estructura. La estructura de minucias formada permite medir la fortaleza de las conexiones entre cada una de las minucias

que conforman una tripleta mediante su conexión con la minucia central y con las demás minucias que forman parte de la estructura. Como trabajo futuro se plantea modificar el proceso de extracción y comparación de estructuras identificativas obtenidas de las minucias mediante la utilización de una función para el cálculo probabilístico de la autenticidad de una minucia en la estructura a comparar, además, se pretende integrar este método de representación de la información contenida en las plantillas de minucias a un modelo de protección de plantillas de minucias de huellas dactilares.

Referencias

AHMAD, T. (2013). Shared secret-based key and fingerprint binding scheme.

AHN, D., KONG, S. G., CHUNG, Y.-S., and MOON, K. Y. (2008). Matching with Secure Fingerprint Templates using Non-invertible Transforms. In *Congress on Image and Signal Processing*, pages 29–33.

BELGUECHIL, R., ROSENBERGERZ, C., and AOUDIA, S. A. (2010). Biohashing for securing fingerprint minutiae templates.

BOONCHAISEREE, N. and AREEKUL, V. (2009). Focal point detection based on half concentric lens model for singular point extraction in fingerprint. In *Advances in Biometrics*, pages 637–646. Springer.

DAHIYA, N. and KANT, C. (2012). Biometrics security concerns. In *Second International Conference on Advanced Computing & Communication Technologies*, pages 297–302. IEEE.

GHANY, K. K., HEFNY, H. A., HASSANIEN, A. E., GHALI, N., et al. (2012). A hybrid approach for biometric template security. In *International Conference on Advances in Social Networks Analysis and Mining*, pages 941–942. IEEE.

JAIN, A. K., NANDAKUMAR, K., and NAGAR, A. (2013). Fingerprint template protection: From theory to practice. In *Security and Privacy in Biometrics*, pages 187–214. Springer.

JEFFERS, J. and ARAKALA, A. (2006). Minutiae-based structures for a fuzzy vault. In *2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, pages 1–6. IEEE.

JEFFERS, J. and ARAKALA, A. (2007). Fingerprint alignment for a minutiae-based fuzzy vault. In *Biometrics Symposium, 2007*, pages 1–6. IEEE.

JIN, A. T. B., LING, D. N. C., and GOH, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11):2245–2255.

JUELS, A. and SUDAN, M. (2006). A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257.

LI, J., YANG, X., TIAN, J., SHI, P., and LI, P. (2008). Topological structure-based alignment for fingerprint fuzzy vault. In *19th International Conference on Pattern Recognition*, pages 1–4. IEEE.

MALTONI, D., MAIO, D., JAIN, A. K., and PRABHAKAR, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

RATHA, N. K., CHIKKERUR, S., CONNELL, J. H., and BOLLE, R. M. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572.

ULUDAG, U., PANKANTI, S., and JAIN, A. K. (2005). Fuzzy vault for fingerprints. In *Audio-and Video-Based Biometric Person Authentication*, pages 310–319. Springer.

WANG, S. and HU, J. (2014). Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 47(3):1321–1329.

XI, K. and HU, J. (2009). Biometric Mobile Template Protection : A Composite Feature based Fingerprint Fuzzy Vault. In *IEEE ICC*, pages 1–5.

ZHANG, X., FENG, Q., and HE, K. (2014). A new blind fingerprint alignment algorithm used in biometric encryption. In *2014 International Conference on Computer, Communications and Information Technology*. Atlantis Press.

ZHE, J. and JIN, A. T. B. (2011). Fingerprint template protection with minutia vicinity decomposition. In *International Joint Conference on Biometrics*, pages 1–7. IEEE.