International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 16 No. 2 Jun. 2016, pp. 349-355

http://www.ijias.issr-journals.org/

Hybrid models for fingerprint minutiae templates protection alignment free

Ramón Santana Fernández[1], Gary Xavier Reyes Zambrano[2], Yanio Hernández Heredia[3], and Adrián Alberto Machado Cento[3]

[1]Biometric research, University of Informatics Science, Havana, Cuba

[2]Facultad de Ciencias Matemática y Física, Universidad de Guayaquil, Guayaquil, Ecuador

[3]Software development, University of Informatics Science, Havana, Cuba

ABSTRACT: People recognition through biometric identifiers has a variety of applications today. This process is performed in plain text, which endangers the safety of data transmitted during the recognition process when performed in low security networks. Biometric identifiers are unique and invariant in the lifetime of an individual. Therefore, once the data associated with the biometric identifier are obtained, it cannot be safely use as a security mechanism, so is not possible to change it as a password or a personal identification number. For the cryptographic protection of biometric data, several models have been proposed, however, problems such as data alignment and the revocation of compromised templates during an attack have not been efficiently addressed in these models. A set of hybrid models have been proposed in the literature to facilitate the revocation and to introduce a contribution to remove the alignment process. For this end, several minutiae structures extraction mechanisms are involved, with the purpose of obtaining a model that uses a method for extracting information invariant to rotation and translation, resistant to nonlinear deformation and partial overlapping and one of the biometric cryptosystems to ensure the extracted set of data.

KEYWORDS: biometric cryptosystems, bio-cryptography, biometric protection free of alignment, minutiae structures, biometric security.

1 INTRODUCTION

Biometrics is the science field which studies people identification methods, using physical and behavioral traits. In [1] biometrics is defined as the measurement of biological data. The process of people biometric identification begins with the acquisition of the biometric feature, features extraction and ends with the comparison of the extracted features with those stored in the database. This process currently takes place in plain text, which constitutes a security problem when biometric data travel in low security networks.

To protect biometric data several models have been proposed in the literature [2]–[4]. These models are the cryptographic foundation for biometric templates protection, however, do not take into account different variations shown during fingerprint sample acquisition. The variations are:

1. Rotation
2. Translation
3. Partial overlapping
4. Nonlinear deformation

These variations hinder the comparison process, so it is necessary to align the minutiae templates before comparing. When the minutiae templates comparison is performed in plain text, templates can be aligned by checking the coordinate and angle of each minutia. Once encrypted minutiae templates, it is not possible to have these features, making the

alignment process a challenge [5]. The main reason lies in the absence of the original features. The comparison in the protected domain is performed using transformed data by an encryption method. The difficulty lies in the change that occurs in the position and angle of the minutiae, and due to is not possible to have the original template, makes difficult to detect which minutiae coincide and which ones are added in the process of fingerprint capture.

For aligning the minutiae templates before performing encryption, various methods have been proposed among which highlight:

- Fingerprint singularities detection [6].
- Focal point detection [5].
- Minutiae reference selection [7].
- The calculation of the iterative closest point [8]–[10].
- The formation of topological structures [11]–[13].

The proposed methods perform the alignment process, however, they present a number of limitations that affect the biometric performance of the minutiae templates protection models which use them. The absence of singularities (core and delta) in fingerprint images precludes the use of the alignment model using the singularities of the fingerprint.

During the process of selecting the focal point or the reference minutiae, the slightest change or failure would lead to an erroneous selection and thus to a significant loss in biometric performance. The inclusion or elimination of minutiae during capture and extraction process, cause instability in the topological structures composing the alignment, besides, storing some data structures as support for the alignment process is considered a security leak.

Some protection models approaches use a set of features extracted from the topological structures to perform the encryption process alignment free. In this case, the problem of changing the minutiae between two extractions of the same biometric trait persists, degrading biometric performance.

This research analyzes hybrid models for minutiae templates protection, making emphasis on the representation methods of the information contained in the minutiae. the structures used to represent information and data extracted for people identification in the protected domain are also analyzed. The article is structured as follows: a study of the state of the art of hybrid models for minutiae templates protection is performed in section 2, the weaknesses of these models are discussed in section 3 and conclusions and future work are discussed in section 4.

2 HYBRID MODELS FOR MINUTIAE TEMPLATES PROTECTION ALIGNMENT FREE

Fingerprints minutiae templates protection models are classified into two groups, the dependents of a method for data alignment and alignment free. Models that include alienation methods [9]–[11] store a set of data called support data; this constitutes a vulnerability because unencrypted data is stored which can be used for correlation attacks. Alignment free models perform the encryption of a set of features from the minutiae, invariant to rotation, translation and nonlinear deformation resistant, encrypting all available information. Cryptographic security in alignment free models is greater because they do not leave unencrypted information. This makes it more complex to correlate different protected minutiae templates belonging to the same biometric trait.

To perform the representation and extraction of features invariant to rotation and translation from the minutiae, in [11] are proposed three topological structures. The proposed structures are:

1. The n-nearest neighbors structure
2. Voronoi diagrams
3. Minutiae Triplets

The research performed in [14] shows the superiority of minutiae triplets and Voronoi diagrams for minutiae templates alignment in plain text. For the cipher text it is not possible to align minutiae templates once they have been encrypted, because of the transformations applied to each component of a minutiae.

To perform the comparison process is necessary to have two pre-aligned templates or a set of data invariant to the rotation and translation suffered by fingerprints during biometric feature data acquisition. To obtain this set of special features, one of the structures proposed by [11] is formed and from it, a set of data from the minutia is extracted. This data is used to perform the encryption process using fuzzy vault models, cancelable templates or biometric hash. These models are considered the cryptographic foundation hybrid models for minutiae templates protection.

In [15] a hybrid models for minutiae templates protection is described. To obtain the features invariant to rotation and translation, a method of representing the information contained in the minutiae is described. The encryption process is performed using the invertible templates model, specifically the Cartesian transformations. The process of invariant features extraction begins with the selection of three minutiae from the minutiae template, then a circle with the minutiae on the edge is formed, the circumcenter of the triplet and the angles formed between each vertex the triangle and the circumcenter is calculated. The encryption process of the identificative characteristics consists in the storage as shown in Figure 1:

1. circumcenter coordinates $(x'; y')$
2. the largest angle φ_{12} and its neighbor or adjacent angle φ_{23}
3. angles $\phi_1,\ \phi_2, \phi_3$
4. minutiae type δ

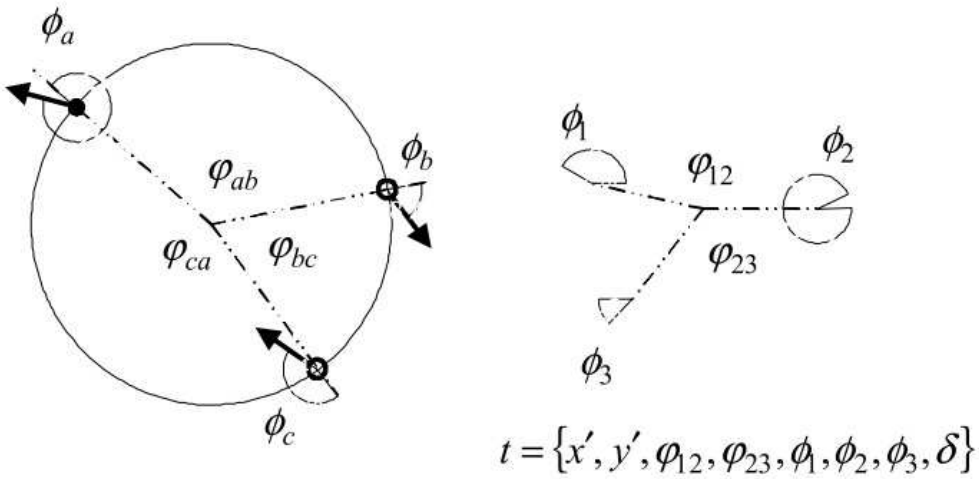

Fig. 1. Extraction identificative characteristics from the center

In [16] a hybrid encryption model for fingerprint biometric data is described. This model consists of a complex feature, invariant to rotation and translation, and a variation of the fuzzy vault encryption model. The given feature is defined as the relation between two minutiae expressed by the length of the line that separates them, the difference of orientation angles of each minutiae and the angle formed by parallel lines to the direction of the minutiae.

The relationships between minutiae is determined using structures of n nearest neighborhood, with n = 4. A 4-dimensional vector, invariant to rotation and translation, which is encrypted using the fuzzy vault model and compared by the hierarchical structure check algorithm (HSC) proposed in this same investigation is formed. Figure 2 shows the structure with each of the extracted features.

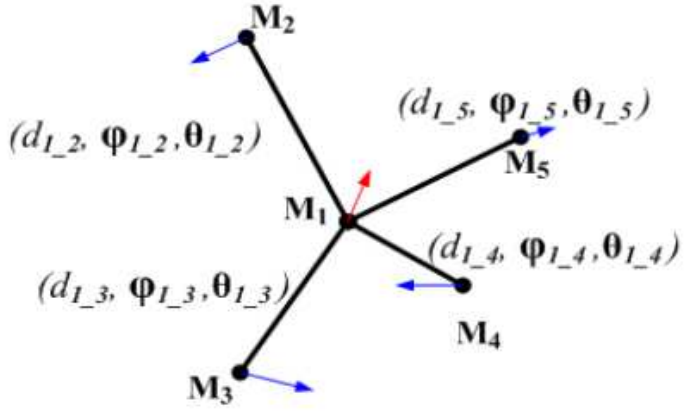

Fig. 2. Compose structure

Another protection hybrid model proposed in [13] formulates a method of representation and extraction of identificative characteristics from fingerprint minutiae triplets. This hybrid model uses a variation of the biometric hash called salting [17] to perform encryption of the extracted features. The process consists of four steps:

1. Minutiae neighborhoods Formulation
2. Neighborhoods Decomposition.
3. Invariant features Extraction
4. Templates Protection.

The formulation of minutiae neighborhoods is done by selecting the 3 closest minutiae (measured by the Euclidean distance) to the m minutia being analyzed. The decomposition process consists in the creation of 4 minutiae triplets, 3 formed by joining the m minutiae and two neighborhoods and the last one formed by their neighborhoods as shown in Figure 3.

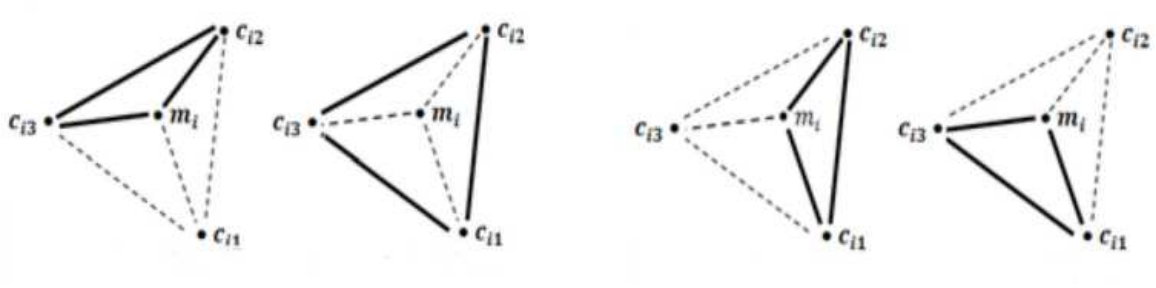

Fig. 3. Minutiae triplet

The process of invariant features extraction takes from each triplet the length of the sides, the amplitude of the inner angles and calculates the difference between the two adjacent minutiae on each side. With these features the characteristic vector is formed to perform encoding.

In [18] this representation and identificative characteristics extraction scheme from the minutiae is used, to perform encryption with cancellable templates model. The matching process is performed by collating all 9 dimensions protected vectors.

In [19] a minutiae templates hybrid protection model is described, which performs the extraction process of invariant features using a structure derived from the Delaunay triangulation called Delaunay quad. The base minutiae structure to form the Delaunay quad is the Voronoi diagram or structure. The method presents the generation of Voronoi diagram associated with a minutiae template and the centers of each neighboring minutiae pair come together to create the Delaunay network. To form Delaunay quadrangles, it is considered a restriction, only two triangles that share one side are selected.

This approach records the local information of the formed topological structures and contains a side and an angle more than what was recorded in the Delaunay triangulation. In this way global information registration is avoided. The main advantage over Delaunay triangulation, this approach proposes greater robustness regarding nonlinear distortion variation. The invariant features selected in this method are:

1. The sides length.
2. The angles between the direction of each minutiae and the corresponding side to its neighbor clockwise.
3. Angles bewteen 2 sides.
4. The type of each minutia.

Each vector extracted from a Delaunay quad is quantized in a short binary string and then all strings are concatenated into a single feature vector of fixed length. To increase the discriminative power of this structure, an additional feature of each Delaunay quad is obtained. For this, the center of each structure is selected and it is considered the reference point or center point to convert the Cartesian coordinates structure to polar coordinates. From each minutia, the radial distance, angular distance and orientation relative to the center is registered. To reduce the effect of nonlinear distortion a quantization process is performed in every minutia.

In [20] a method for representation and extraction of information contained in the minutiae template is described. The method is invariant to rotation and translation and it is called minutiae shell. The proposed method consists of 3 stages:

1. Extraction of the core and delta singular points.
2. The calculation of the distance of each minutia to the singularities.
3. The construction of the minutiae shell.

Calculating the distance of each minutia to the singularities is performed using the Euclidean distance measure and the construction of the minutiae shell/curve. This consists in the construction of right triangles where the calculated distances match the hypotenuse of the triangle. To construct the first triangle, initial distance d_0 is randomly generated, which is the private key of each user where (a) shows on the left, the distance between the points and the center; the center shows the creation of the minutiae shell and the right shows the curve formed by the union of the triangles of the minutiae shell. This method is proposed by its authors as an encryption model, however, it does not meet the basic requirements to be considered as such.

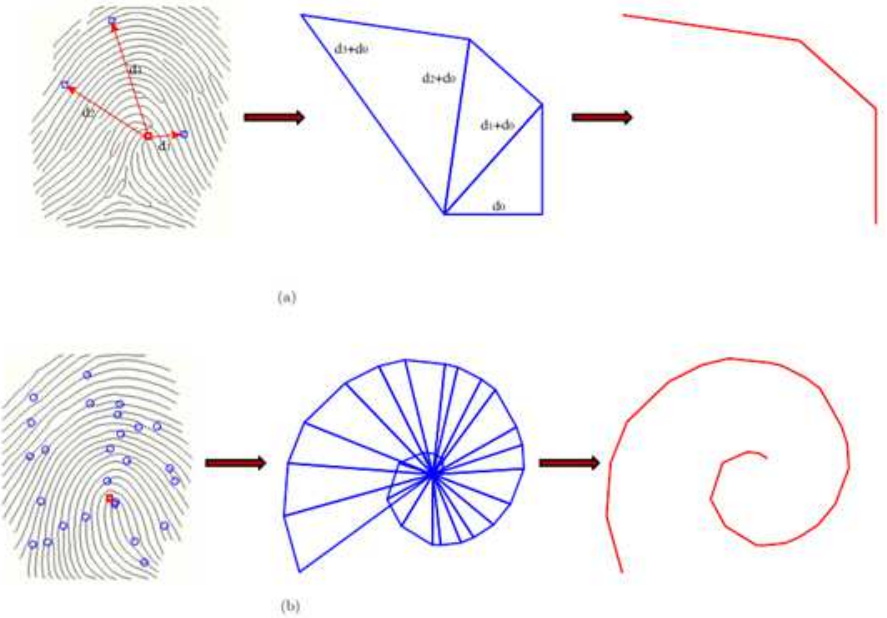

Fig. 4. Minutiae structure centered at the core of the fingerprint

In [21] a form of representation of the information contained in the minutiae templates is described, based on the comparison method called Minutia Cylinder-Code (MCC) for encrypting the data using the cancellable templates model. In this contribution, the same representation method is used as described in [22].

After obtaining the MCC cylinders the combined plate technique (CP) is performed, which involves the generation of combined pre-plates (PCP) from parts of the original MCC. Each PCP is combined by XOR with randomly generated boards (RP), which constitute the private key of the user. These two steps are the generation of CP which is comprised of a vector of two bits CP $\in$ {0,1}. Each CP is protected using the cancellable templates encryption model, by any of the three transformations it proposes.

In [23] a method of representation and extraction of identificative characteristics is proposed, invariant to rotation and translation, resistant to nonlinear deformation and partial overlapping. This representation method can be used by any of the pioneering models for alignment free encryption of biometric data from fingerprints. The extraction process of identificative characteristics and representation is composed of:

1. Formation of the minutiae complex structure.
    a. Selection of the 5 nearest neighborhoods.
    b. Extraction of minutiae triplets that can be formed using the center and neighboring minutiae of the structure.
2. Extraction of identificatives features
3. Classification of the extracted features

The features extracted to make the encryption process using fuzzy vault or cancellable templates are:

1. The sides length
2. The amplitude of the inner angles.
3. The difference between two adjacent angles aside.

Representation methods analyzed in this research performs representation and extraction of identificative information of the minutiae and prepare data for the encryption process taking into account the non-linear distortion, rotation and translation of data. Efforts in each approach are intended to solve the problem of minutiae templates alignment and to increase the strength of the method regarding the minutiae change by insertion or deletion in a set relative to another one.

3 ANALYSIS OF HYBRID MODELS FOR MINUTIAE TEMPLATES PROTECTION ALIGNMENT FREE

The analyzed models perform data encryption and allow comparison of minutiae templates in the encryption domain without making the data alignment process. All models analyzed perform the transformation of the original biometric data (minutiae) into a set of data invariant to rotation and translation, resistant to nonlinear deformation and partial overlapping experienced by fingerprints during capture or data acquisition. This initial process mitigates one of the vulnerabilities presented by pioneering models to encrypt all data and delete data support.

For the comparison of minutiae templates in the protected domain, it is required a set of attributes (or important considerations) which are:

1. Minutiae templates alignment.
2. Comparison in the protected domain.
3. Global and Local analysis of the information contained in protected templates.

The analysis showed the need for a comparison mechanism to analyze the information obtained during the representation and extraction of invariants identificative characteristics process both globally and locally. Hybrid models only provide the possibility of eliminating the alignment process, improving one vulnerability aspect of the cryptographic models proposed for this purpose. As a result of the analysis of the hybrid models for minutiae template protection, weaknesses that undermine the cryptographic security, revocation and performance of minutiae templates protection models were detected. They are detailed below:

1. Hybrid models have the same vulnerabilities of pioneering models (fuzzy vault, cancelable templates and biometric hash) because they only perform an initial transformation of the data to eliminate the need to align the templates during the comparison process.
2. The absence of an approach to predict with some certainty degree when a minutia forming a topological structure is considered a negative effect on the biometric performance of the models.
3. The revocation of protected templates is complex to achieve; in most cases it is necessary to change the encryption function as discussed in the pioneering models.
4. Some models proposed as encryption models are just methods of representation of the information contained in the minutiae templates lacking revocation.

4 CONCLUSION

Selecting a set of techniques for extracting identificative characteristics invariant to rotation and translation, resistant to nonlinear deformation and partial overlapping, allowed to eliminate security breaches persistent in the support data. The models used to encrypt the biometric data extracted from minutiae, have vulnerabilities that persist in the analyzed hybrid models. The analysis of the characteristics used for the representation of the information contained in the minutiae, improved understanding of the invariant element used to perform encryption and comparison in the protected domain. As future work is planned to use the complex structure to develop a hybrid model for Fingerprint minutiae templates protection alignment free.

REFERENCES

[1] N. Dahiya and C. Kant, "Biometrics Security Concerns," in *Second International Conference on Advanced Computing & Communication Technologies Biometrics*, 2012, pp. 299–304.

[2] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28–36.

[3] R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," vol. 40, no. 3, 2001.

[4] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in *IEEE International Symposium on Information Theory*, 2002, p. 408.

[5] K. Nandakumar, "A Fingerprint Cryptosystem Based on Minutiae Phase Spectrum," pp. 2–7, 2010.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. 2009, p. 506.

[7] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 236–246, 2010.

[8] X. Zhang, Q. Feng, and K. He, "A New Blind Fingerprint Alignment Algorithm used in Biometric Encryption," in *International Conference on Computer, Communications and Information Technology*, 2014, vol. 1, no. Ccit, pp. 231–234.

[9] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-Based Fuzzy Vault : Implementation and Performance," *IEEE Trans. Inf. FORENSICS Secur.*, vol. 2, no. 4, pp. 744–757, 2007.

[10] U. Uludag, "Securing Fingerprint Template : Fuzzy Vault with Helper Data," in *Conference on Computer Vision and Pattern Recognition Workshop.*, 2006, pp. 163–171.

[11] J. Jeffers and A. Arakala, "FINGERPRINT ALIGNMENT FOR A MINUTIAE-BASED FUZZY VAULT," in *Biometrics Symposium*, 2007.

[12] J. Li, X. Yang, J. Tian, P. Shi, and P. Li, "Topological Structure-based Alignment for Fingerprint Fuzzy Vault," in *19th International Conference on Pattern Recognition, 2008. ICPR 2008.*, 2008, no. 1, pp. 1–4.

[13] J. Zhe and A. T. Beng Jin, "Fingerprint Template Protection with Minutia Vicinity Decomposition," in *International Joint Conference on Biometrics*, 2011, pp. 1–7.

[14] A. Arakala and J. Jeffers, "Minutiae-Based Structures for a Fuzzy Vault," in *2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, 2006, pp. 1–4.

[15] D. Ahn, S. G. Kong, Y. Chung, and K. Y. Moon, "Matching with Secure Fingerprint Templates using Non-invertible Transforms," pp. 29–33, 2008.

[16] K. Xi and J. Hu, "Biometric Mobile Template Protection : A Composite Feature based Fingerprint Fuzzy Vault," pp. 1–5, 2009.

[17] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," vol. 2008, 2008.

[18] Z. Jin, B.-M. Goi, A. Teoh, and Y. H. Tay, "A two-dimensional random projected minutiae vicinity decomposition-based cancellable fingerprint template," *Secur. Commun. Networks*, vol. 7, no. 11, pp. 1691–1701, 2014.

[19] W. Yang, J. Hu, and S. Wang, "A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Using Topology Code for Local Registration and Security Enhancement," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1179–1192, 2014.

[20] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, "Fingerprint shell : Secure representation of fingerprint template q," *Pattern Recognit. Lett.*, vol. 45, pp. 189–196, 2014.

[21] N. Zhang, X. Yang, Y. Zang, X. Jia, and J. Tian, "Generating Registration-Free Cancelable Fingerprint Templates Based on Minutia Cylinder-Code Representation."

[22] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia Cylinder-Code : A New Representation and Matching Technique for Fingerprint Recognition," vol. 32, no. 12, pp. 2128–2141, 2010.

[23] R. S. Fernández, A. A. M. Cento, and V. E. Sentí, "Method for minutiae representation and identifying information extraction on fingerprint templates," *Rev. Cuba. Ciencias Informáticas*, vol. 9, no. 4, pp. 132–141, 2015.