International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 11007-11014

Biometric Protection Approach Based on Fingerprint Hierarchical Identification

Meryam Elmouhtadi
Department of physics, LRIT – CNRST URAC29, Faculty of Sciences, Mohammed V University in Rabat, Morocco.
Orcid Id: 0000-0002-5089-0860

Maryam Lafkih
Department of Physics, LRIT – CNRST URAC29, Faculty of Sciences, Mohammed V University in Rabat, Morocco.

Sanaa El fkihi
RIITM, ENSIAS, University Mohammed V Rabat, Morocco.

Abstract

With the exponential increase in the dependence on biometric based fingerprint in everyday life, there is a growing concern related to privacy and security issues; therefore, security threats need tobe analyzed in detail. Different fingerprint systems store personal information without any security. Hence, an attacker can easily have access to the identity of legitimate user. In order to secure these applications against different threats, several protection approaches have been proposed as alternative solution. In this paper, we propose a new approach for fingerprint template protection based on the fingerprint features transformation. In this context, we proposed a new indexation approach named 'Hierarchical Identification and Protection Approach Based on Delaunay Triangulation', based on the topological transformation of minutia points. First, we applied the Delaunay triangulation as a matching method. Then we introduced the barycenter notion, which applied on the similar extracted triangle. This hierarchical meaner of triangulation improve the performance and the security of fingerprint systems. Driven experimental results show the ability of the proposed approach to preserve the performance and the security of biometric authentication systems.

Keywords: Fingerprints indexation, biometric template protection, security

INTRODUCTION

Fingerprint recognition refers to the automated method of identifying or verifying the individual identity based on the comparison of two fingerprints. It is one of the most well used biometrics system, and by far the most used solution for authentication on computerized systems [1]. It has been extensively used by forensic in criminal investigations or in the security systems. The uniqueness of a fingerprint is determined by the representation of its ridge structure and the presence of certain ridge form called minutiae points. Their positions are key factors to differentiate between individual's templates [2].

Biometric based fingerprint recognition systems are divided in two categories: verification and identification. The verification system is based on the one to one comparison between an enrolled fingerprint stored in the database and an input fingerprint that is the subject of a request. The identification is considered as one to many comparisons (between request fingerprint and stored database). The fingerprint comparison and matching involves using the indexation methods to extract the important features. The performance and the security of biometric systems depend on several factors such as indexation methods and the robustness against different attacks

The indexing methods used in biometric systems have a very important factor on the biometric system performance[1][3].In terms of fingerprint indexing, we find two fundamental approaches in literature: methods based on the general form represented by papillary ridges of the fingerprint and methods based on the extraction of the main minutiae features extracted from the fingerprint impression, like orientation, Euclidean distance, number and location[4]. The best indexing systems have proven that approaches based on minutiae gives better results compared to others.

On the other hand, an attacker can exploit several threats and attacks (e.g. spoofing, falsification and alteration attacks) in order to gain illegitimate access to the biometric system; he can use the obliteration, distortion and the imitation [5][6] to get around to the biometric system. Besides data is not always secret, which increase the vulnerabilities of biometric templates. For example, in the case of fingerprint features, an attacker using touched object can reproduce the biometric data. This type of alteration has direct relation with used

indexation methods, where an attacker can easily gain access to the system if it uses indexation method with low performance[7].

Despite the active research carried out in recent years to protect biometric template, the relation between the indexation method and the security of fingerprint biometric systems is not yet investigated. Hence, this paper is concerned with the proposition of a new performed indexation method based on Delaunay triangulation. The proposed method ensures an increase in the biometric system's fingerprint performance and security against modification attacks (e.g. blurry images).

The remainder of this paper is organized as follows: the related work is presented in Section II, the proposed system and the details stages are explained in Section III. Results and discussion are introduced in Section IV. Finally, the conclusion and future work are presented in Section V.

RELATED WORKS

1) Features Transformations

Security has become increasingly a concern in biometric systems; it ensures confidentiality by providing a robust authentication process against any type of deception and also against the possibility of raising the original biometric characteristics [8]. For this purpose, features transformations are proposed as biometric template protection technique. These methods are based on applying a transform function on the biometric characteristics. Instead of the biometric characteristics, the transformed characteristics will be stored in the database as a reference model. The same transformation is applied to the query during authentication and then matched with the stored template [9].

A several template transformation methods have been proposed and classified into two classes:(i) Transformation based on vector and (ii) Transformation based on interest point [10]. In the first methods, the biometric template is represented as a vector, to compute the dissimilarity, the used Euclidean distance. Biohashing is an example of this class; in this method, the features vector is multiplied with an orthogonal transformation matrix. However, Biohashing is easy to invert when the key is known to the attacker, which degrades the performance of this method.

BioPhasor is considered as improvement of the biohashing, in this method a set of complex vectors is obtained using the biometric vector and the orthogonal transformation (used as imaginary part). Although, this scheme is considered as more secure tan Biohasing, the complexity to inverting this transformation is not known.

Many Fingerprint features are represented by a set of points (minutiae) [11]. Ratha et al used Cartesian, polar and functional transformation.Whereas in the Cartesian case, the fingerprint is transformed into a set of rectangles which placed following the associated key. In the polar transformation, the fingerprints are divided into of shells and each oneis divided into sectors. In case of the functional transformation, 2D Gaussians and electric potential field in 2D charge distribution are applied to obtain the translation corresponding to the minutia. However, the performance is reducing due to an increase in the intra-user variations. Besides, these transformations require the alignment of fingerprints before the transformation.

In order to prevent the weaknesses of these transformation methods, we will propose in this paper a new approach based on the triangular transformation of the extracted minutes. Instead of using an external secret key, our approach is based on the extraction of the secret key from the biometric features in order to increase the security of the proposed system. We use the angles of the first generated triangles as a secret key to perform the second transformation.

2) Indexing

Fingerprint matching consists to compare and calculate the similarity index, then generating a match score of two fingerprints for verification or identification procedures. This index is calculated basing on an indexing method, which is the main challenge of fingerprints recognition. Literature divides the fingerprint matching algorithms in two different classes: (i) correlation-based methods and (ii) minutiae-based methods. Correlation-based methods compute the correspondence of two super imposed fingerprints, by seeking the correlation from pixels in the two images in different alignments, regardless of their forms or characteristics. Due to nature of skin, these methods are not robust to the major fingerprints image problems, because pixels displacements that make two impressions of the same finger very different, skin conditions on the sensing time and contrast /brightness can add/eliminate ridges or changing the fingerprint characteristics. In case of rotated fingerprint, computation of the cross-correlation for different angles is computationally inefficient [1] [12].

Hence, it is necessary to apply a set of treatments on fingerprint images in order to make it ready for use and also to keep the useful information.

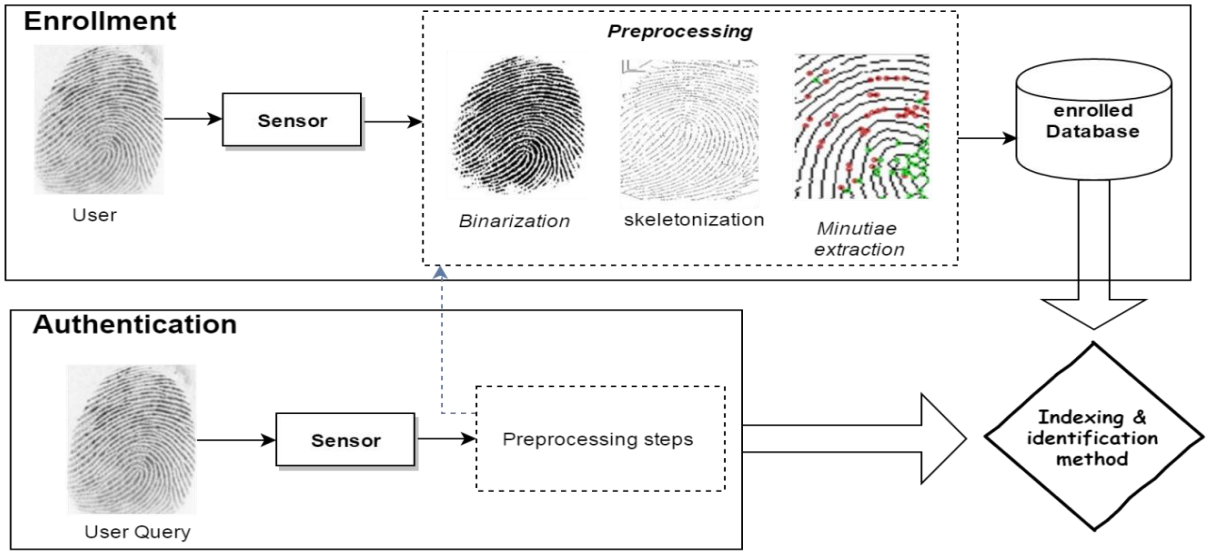

Figure 1: Fingerprint indexing steps.

Several studies have been established in this context. In general, all indexing approaches based on minutiae characteristics are based on the three main preprocessing steps: (i) binarization, (ii) skeletonization and (iii) minutiae extraction as shown in Fig. 1.Other approaches use the directional field, which consists to calculate the direction of each extracted minutiae using the gradient method, then the obtained information will be used in the indexing process. In our case, we rely on thethree steps based method that we detail bellow:

- **Segmentation or binarization**: it consists of derive the shape of ridges and remove the background pixels before extracting minutiae. The commonly used approach is segmentation by adaptive or global thresholding. In our case, we opt for the segmentation method developed by Otsu [13]. It allows maximizing the interclass variation defined as a weighted sum of variances of the two classes; more this variance is high, more the threshold is able to segment the image correctly.
- **Skeletonization**: Consist to reduce the thickness of ridges in a line of one pixel in order to facilitate minutiae extraction. We use the Zhang approach [14] that proved significant results, as demonstrated in [15].
- **Extraction of minutiae**: Consist to extract terminations and bifurcations as the most significant features in a fingerprint impression. In all most approaches, the extraction is made by dividing the skeletonized image into blocks (Fig. 2). To improve the extraction process and eliminate false extracted minutiae, approaches such as [16] consider a Cross Number (CN); on a neighborhood of 8 pixels. The center pixel is the location of a bifurcation when the crossing number is equal or greater than three, then it present isolated point when the crossing number is null, and it is a not considered as a minutiae point.

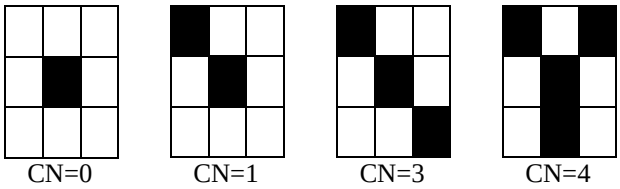

Figure 2: Examples of CrossNumber

- CN=0; Isolated pixel, not considered (due to a noise).
- CN=1; ridge minutiae.
- CN=2; minutiae not exist.
- CN=3; bifurcation.

3) Delaunay Triangulation

As a minutiae-based matching, we consider the matching based on minutiae triangulation, which is an effective tool to deal with discrete data comparison and still a suitable method to treat a set of dispersed data. Hence, each three minutiae form a triangle that keeps topological structures of them which gives a great progress in the matching and indexing algorithms.

Matchers based on triangulation gives a higher quality comparing to other minutiae based methods. They have the following advantages:

- They are robust to fingerprint deformations, like translation, rotation dispersion and missed regions [17].
- They are more accurate and less complex, compared to algorithms based on other features [18].
- Minutiae triplets have higher discriminative power than minutiae pairs and single minutiae[19].
- Considering local points, triangulation is robust to the quality of fingerprint image. Whatever the quality of the sensor, the accuracy of matching will remain elevated.
- Compared with most methods that rely on rigid transformation assumptions, Delaunay triangulation make systems more robust and computationally efficient[20].

Delaunay triangulation method [18][19]and [21] consists to generate the largest possible number of triangles formed by the extracted minutiae points. The problem is that the number of the generated triangles may be a weakness for these algorithms. Indeed, as the set of extracted minutiae points may contain false ones, so for each false minutia, multiple false triangles will be generated, then the matching rate will decrease. Other approaches [18][22] propose to reduce the number of the generated triangles, but this is not efficient as it can delete important minutiae points. Odors approaches are based on the characteristics formed by the obtained triangles [22], such as the lengths of arcs, the nails or the surfaces of triangles; this can reduce the matching time but are not tolerant for all minutiae transformations and decreases the performances. Therefore, how can we increase the matching rate while using relevant triangles?

PROPOSED APPROACH

As a fingerprint matching method, we propose a new approach based minutiae triplets to improve fingerprint recognition in term of accuracy and security. Based on hierarchical Delaunay triangulation, this method uses the triplets of the extracted minutiae as a key for a first comparison. Then a new method based barycenter extraction will beused to ensure the location of similar triplets. Fig.3shows an overview of the proposed matching method.

To compare two fingerprints, we consider a query finger (*Finger1*) and user finger (*Finger2*). The first step of our approach consists to apply the preprocessing steps to each image in order to extract minutiae. Extracted minutiae will be stored into a vector (*ridges* and*bifurcations*).

The preprocessing steps contains (i) binarization based on Otsu's method[13], (ii) the Zhang's approach for skeletonization [14][15], and (iii) the Cross Number based method [16] in order to extract the minutiae points. Based on the obtained minutiae vectors ***M1*** (from *Finger1*), and ***M2*** (from *Finger2*) we generate the different possible triangles using Delaunay triangulation method. The obtained results are saved in ***DT1*** and ***DT2*** that represent the triangles set for query and user fingerprints respectively. Using a matching process, we aim to calculate the similarity of the both fingerprints using the triangles features for indexing fingerprints. To this end, we calculate the three angles of each triangle obtained in ***DT1*** and ***DT2***. Among the existing methods, we use the Al-Kashi theorem (eqs. (2), (3), and (4)) to define the three angles: α_1, $\alpha_2$andα_3 of each triangle in ***DT1***, ***DT2*** (see Fig. 4).

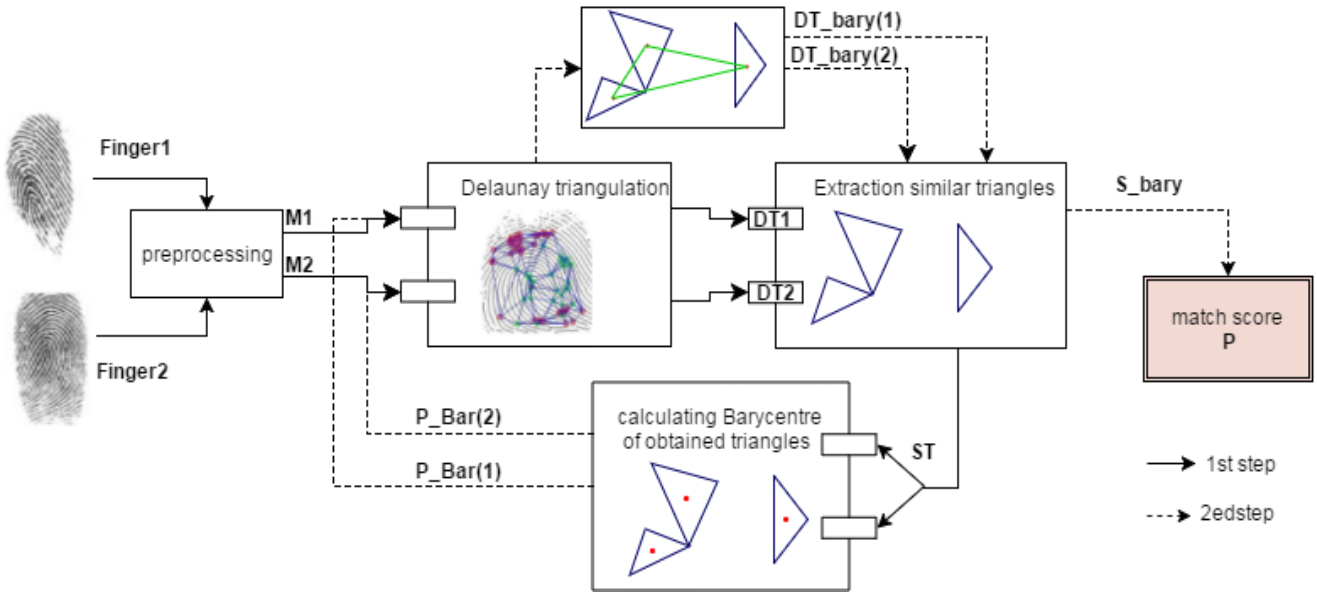

Figure 3: Proposed approach

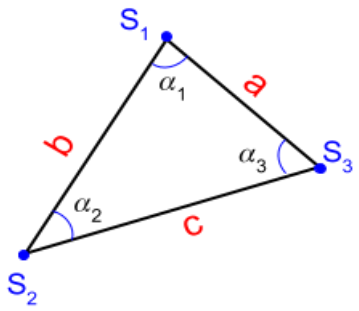

Figure 4: An example of a triangle

$$\alpha_1 = \arccos\left(\frac{a^2+b^2-c^2}{2ab}\right) \quad (2)$$

$$\alpha_2 = \arccos\left(\frac{b^2+c^2-a^2}{2bc}\right) \quad (3)$$

$$\alpha_3 = \arccos\left(\frac{a^2+c^2-b^2}{2ac}\right) \quad (4)$$

As a first step, we compare the triangles obtained with the both compared fingerprint using their angles, then similar triangles results will be saved in ***ST***. In this step, we may find similar triangles that are not formed by the same minutiae. Indeed, despite the existence of a homothetic transformation between two triangles, it does not really guarantee their similarity; because they can be in two different positions into compared fingerprints. Then it is not sufficient to give a good similarity rate. To deal with this problem and to take into consideration the geometric location of similar triangles, the second process of our approach consists to extract the barycenter of each triangle given in ***ST***. The barycenter is calculated by using the coordinates mean of the nodes of each triangle $\Delta_i(S_{1i}, S_{2i}, S_{3i})$ given in ***ST***(eqs.(5),(6)), where$\{S_{i(x,y)}: i = 1,2,3\}$ are the minutiae coordinates, the result will besaved in ***P_Bar (P_Bar_x, P_Bar_y)***.

$$P\_Bar\_x = \frac{S_{1x}+S_{2x}+S_{3x}}{3} \quad (5)$$

$$P\_Bar\_y = \frac{S_{1y}+S_{2y}+S_{3y}}{3} \quad (6)$$

We apply the Delaunay Triangulation ***DT_bary*** of points saved in the vector ***P_Bar***. For each three similar triangles, we generate a triangle such its nodes are the centroids of the three considered triangles. Then, we seek for the similar triangles of centroids. This method will ensure improvement regarding the similarity decision of triangles. Then we measure the similarity between ***DT_bary(1)*** of the query fingerprint and ***DT_bary(2)*** of the user fingerprint.

The probability of identification (***P***) of each query fingerprint compared to the database images is defined as follows:

$$P_1 = \frac{|ST|}{|DT|} \quad (7)$$

$$P_2 = \frac{|S\_bary|}{|DT\_bary(1)|} \quad (8)$$

$$P = P_1 * P_2 \quad (9)$$

|DT|: Cardinal of triangles obtained in the first time with Delaunay triangulation.

|ST|: Cardinal of similar triangles obtained in the first comparison.

|DT_bary(1)|: Cardinal of similar triangles obtained using Delaunay triangulation of barycenter points.

|S_bary|: Cardinal of similar triangles obtained using Delaunay triangulation of barycenter points.

As mentioned above, the proposed indexation method is considered also as biometric system protection approach based on features transformation techniques. Where the barycenter is used as transformation method and the three angles of the first triangle areconsidered as secret key which considered as confidential information.

In order to evaluate the proposed approach, we tested our system against altered images; this can explain the impact of the image degradation on the proposed approach in terms of performance and security.

Original blur

Figure 5: Example of original and burred image

Blurred images are used as type of alteration; hence we evaluate the proposed system under the blur degradation. Blurred images are generated based on the 2D Wiener filter, using several variations of the blur. Fig. 5 presents an example of original and blurred images. Besides, to show the performance of the proposed approach against intra-class and inter-class variation, the system is tested using both the verification and identification scenarios. In the first case, we compare the request image of the user with all the stored images of the same user where in the second case; each user image is compared with the database.

The alteration images allow evaluating our approach on two points:

1. The performance of the proposed method under signal degradation.
2. The security of the proposed approach against attack using altered images where the attacker present to the system altered images of real user [23].

EXPERIMENT AND RESULTS

This section presents all the experimental study and the obtained results. Subsection 1 describes the hardware and software environment used in our experiments. Subsection 2 details the used data sets. Subsection 3, shows the experiments of our algorithm and discusses the obtained results.

1) Hardwares and softwares

The experiments were performed on a desktop personal computer (PC) with the following features:

- Processor: Intel® Core™ i5-3230M
- Clock speed: 2.60 GHz
- Cache: 8 MB
- RAM: 4 GB
- Operating system: Microsoft Windows 10 x64
- Programming languages: MATLAB.
- Softwares: MATLAB R2014b.

2) Dataset

To evaluate the performance of the proposed method, we use the dataset DB1_B from FVC2002 database available at [24]. FVC2002 DB1 and DB2 contain 880 fingerprint impressions, of various quality, from 110 distinct fingers (i.e., each person is represented by 8 impressions). Three different scanners and the SFinGE synthetic generator were used to collect fingerprints (see Table 1).

Table 1: Some information about used database

	Technology	Size	Resolution
DB1	Optical Sensor (CrossMatch V300)	640×480	500 dpi
DB2	Optical Sensor (Digital Persona U.are.U 4000)	328×364	500 dpi
DB3	Thermal Sweeping Sensor (Atmel FingerChip)	300×480	512 dpi
DB4	Synthetic Generator (SFinGe v3.0)	288×384	About 500 dpi

3) Experiments and discuss

First, we evaluate the proposed approach in term of performance. Each user's images tested as reference against blurred images with different levels of blur ([0, 7]). Blurred images are considered as request presented by the real user. Some variations are presented by the attacker who has access to the altered image of the real user (lifted using a mobile trace or a touched object)

Fig. 6 shows the distribution of the matching score according to the alteration level. We notice that the matching score is varied with the level alteration, where the matching scores decrease when the levels increase. Furthermore, we remark that even if the level is minimal (equal to 1), the matching score remains limited, this is due to the two transformation approaches based on barycenter used on our proposal which increase the performance of the system and hamper the acceptation of alteration request that can be used by an attacker to gain illegitimate access.

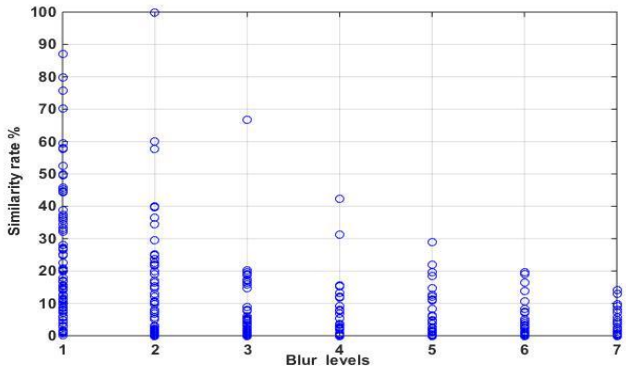

Figure 6: Variation of Fingerprint matching score with blur levels

More details are shown in Table 2, where the matching score differs from user to other; if the level of alteration equals 1, we notice that the score will varied between 45 and 87. This score presents a low percentage of matching for the majority of user images; this can be explained the obtained robustness of the proposed method against the alteration attacks even if the alteration is low.

Table 2: Some matching variation score of different alteration levels.

Level Test	1	2	3	4	5	6	7
1	49,79	36,46	16,49	0	4,61	0	0
2	75,77	60	66,66	42,42	28,78	5,17	09,09
3	70,21	57,65	20,33	12,12	12	0	0
4	87,17	100	0	0	0	0	0
5	52,55	23,76	4,54	2,50	0,89	2,98	3,57
6	59,56	40,07	14,56	8,06	7,04	6,31	5,10
7	45,16	22,58	0	0	0	0	0

In the Fig. 7, we present the Roc (Receive Operating System) curve of our approach. That presents the variation between the false accepted images, which normally identify a false user compared with a not corresponded image. The false positive rate was generated by comparing each user with their seven alterations levels for their different image variations. We can notice that the proposed approach preserves, in general, the performance of the proposed indexing system, which means that hierarchical indexing resists against attacks with a reconstructed image under different levels of alteration.

Finally, since one of the main goals of indexing and identification algorithms is to achieve the speed-up of the identification process, we list in Table 3 the overall time spent on all stages of our algorithm.

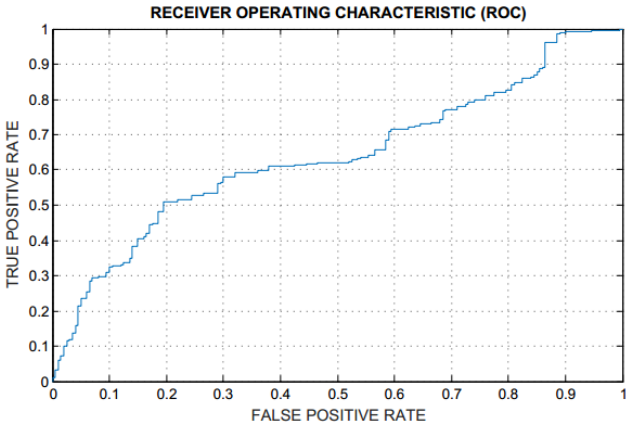

Figure 7: The Roc curve of our approach.

Table 3: Overall time for each stage of the proposed.

Stage in fingerprint indexing and identification	**Time(s)**
Preprocessing steps, minutiae extraction and post processing.	12,98 s
Extracting similar triangles and matching.	2,55 s
Index creation by generating the barycenter triangles.	0,06 s
Average verification of a real user.	11.796 s
Average verification of a blurred user.	19,32 s

CONCLUSION

In this work, we have presented a new approach for fingerprint template protection based on the fingerprint features transformation. In this context, we proposed an indexing method based minutiae triplet and their transformation. This method considered as a biometric system protection that consider the angels of obtained triangles as a secret key that present the confidential information of the fingerprint. We have generated the blurred fingerprints images as a mean of attack alteration. The obtained results present a good toleration of the presented attack from the proposed protection system.

In the future works, we aim to verify the protection system of a different systems attack, as zoom alteration, luminosity, missed pixels and poor-quality alterations. As to prove the performance of our protection system and improved the indexing method for good ends.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable and helpful comments andsuggestions to improve and clarify this paper.

REFERENCES

[1] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of fingerprint recognition.* (springer, 2009).

[2] N. K.Ratha, J. H. Connell, R. M. Bolle, An analysis of minutiae matching strength, *Third International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 223-228, 2001.

[3] Cappelli, R., Maio, D., Maltoni, D., Wayman, J. L., & Jain, A. K. Performance evaluation of fingerprint verification systems. *IEEE transactions on pattern analysis and machine intelligence*, (2006).28(1), 3-18.

[4] Feng, J., & Zhou, J. (2011, November). A performance evaluation of fingerprint minutia descriptors. *In Hand-Based Biometrics (ICHB), IEEE International Conference* on (pp. 1-6).2011.

[5] S. Yoon, J. Feng and A. K.Jain: Altered fingerprints: Analysis and detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol: 34, pp:451-464, 2012.

[6] T. Putte and J. Keuning: *Biometrical fingerprint recognition*: don't get your fingers burned. Smart Card Research and Advanced Applications, pp: 289-303, 2000.

[7] Galbally, J., Fierrez, J., Alonso-Fernandez, F., & Martinez-Diaz, M. Evaluation of direct attacks to fingerprint verification systems. *Telecommunication Systems*, (2011).47(3), 243-254.

[8] Jain, A., Nandakumar, K., and Nagar, A., Biometric template security,(2008) *EURASIP Journal on Advances in Signal Processing*, 1–17 (2008).

[9] Bringer, J. and Chabanne, H., An authentication protocol with encrypted biometric data, in *Proceedings of the Progress in Cryptology,(AFRICACRYPT)*, 109–124 (2008).

[10] Teoh, A. B. J., Goh, A., and Ngo, D. C. L., Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs,*IEEE Transactions on Pattern Analysis and Machine Intelligence* 28, 1892–1901 (December 2006).

[11] Jin, A. T. B., Ling, D. N. C., and Goh, A., Biohashing: two factor authentication featuring fingerprint data and tokenised random number, (2004)*Pattern Recognition* 37(11), 2245–2255

[12] K. Nandakumar, A. K. Jain, Local Correlation-based Fingerprint Matching, in *Proc. ICVGIP, Kolkata*, 2004, Pp. 1 - 6.

[13] M. Sezgin and B. Sankur. Survey over image thresholding techniques and quantitative performance evaluation. (2004) *Journal of Electronic Imaging* 13 (1).pp. 146–165.

[14] J. Parker, Algorithms for Image Processing and Computer Vision, ser. IT Pro. Wiley, 2010.

[15] TISSE, C. L., MARTIN, L., TORRES, L., & ROBERT, M. Système automatique de reconnaissance d'empreintes digitales. Sécurisation de l'authentification sur carte à puce. In *18° Colloque sur le traitement du signal et des images, FRA, 2001. GRETSI, Groupe d'Etudes du Traitement du Signal et des Images.* (2001)

[16] Munoz-Briseno, A. G. Alonso, and J. H. Palancar, Fingerprint indexing with bad quality areas,*Expert Syst. Appl*., vol. 40, no. 5,pp. 1839–1846, 2013.

[17] N. Liu, Y. Yin, and H. Zhang, A fingerprint matching algorithm based on Delaunay triangulation net, in *CIT. IEEE Computer Society*, pp. 591–595, 2005

[18] G. Bebis, T. Deaconu, and M. Georgiopoulos, Fingerprint identification using Delaunay triangulation, in *IEEE International Conference on Intelligence*, Information, and Systems ICIIS, 1999, pp. 452–459.

[19] M. A. Medina-Pérez, M. García-Borroto, A. E. Gutierrez-Rodríguez, & A. Robles, L. Improving fingerprint verification using minutiae triplets, *Sensors*, 12(3), 3418-3437, 2012.

[20] Wang, C., & Gavrilova, M. L. (2006, July). Delaunay triangulation algorithm for fingerprint matching. In *2006*IEEE *3rd International Symposium on Voronoi Diagrams in Science and Engineering* (pp. 208-216).

[21] J. de Boer, A. M. Bazen, and S. H. Gerez, Indexing fingerprint databases based on multiple features,2001.

[22] X. Liang, T. Asano, and A. Bishnu, Distorted fingerprint indexing using minutia detail and delaunay triangle.in *ISVD. IEEE ComputerSociety*, 2006, pp. 217–223.

[23] M. Lafkih, P. Lacharme, C. Rosenberger, M Mikram, S. Ghouzali, M. El Haziti, A Wadood, D. Aboutajdine.

[24] Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002). FVC2002: Second fingerprint verification competition. In Pattern recognition, 2002. *IEEE Proceedings. 16th international conference* on (Vol. 3, pp. 811-814).