Fingerprint Matching and Non-Matching Analysis for Different Tolerance Rotation Degrees in Commercial Matching Algorithms

A. J. Perez-Diaz*[1], I. C. Arronte-Lopez[2]

[1,2] Instituto Tecnológico y de Estudios Superiores de Monterrey,
Campus Cuernavaca
Autopista del Sol KM.104
C.P. 62790
Cuernavaca, Morelos, Mexico
*jesus.arturo.perez@itesm.mx

ABSTRACT

Fingerprint verification is the most important step in the fingerprint-based biometric systems. The matching score is linked to the chance of identifying a person. Nowadays, two fingerprint matching methods are the most popular: the correlation-based method and the minutiae-based method. In this work, three biometric systems were evaluated: Neurotechnology Verifinger 6.0 Extended, Innovatrics IDKit SDK and Griaule Fingerprint SDK 2007. The evaluation was performed according to the experiments of the Fingerprint Verification Competition (FVC). The influence of the fingerprint rotation degrees on false match rate (FMR) and false non-match rate (FNMR) was evaluated. The results showed that the FMR values increase as rotation degrees increase too, meanwhile, the FNMR values decrease. Experimental results demonstrate that Verifinger SDK shows good performance on false non-match testing, with an FNMR mean of 7%, followed by IDKit SDK (6.71% ~ 13.66%) and Fingerprint SDK (50%). However, Fingerprint SDK demonstrates a better performance on false match testing, with an FMR mean of ~0%, followed by Verifinger SDK (7.62% - 9%) and IDKit SDK (above 28%). As result of the experiments, Verifinger SDK had, in general, the best performance. Subsequently, we calculated the regression functions to predict the behavior of FNMR and FMR for different threshold values with different rotation degrees.

Keywords: biometry, fingerprints, matching, rotation, FMR, FNMR.

RESUMEN

La verificación de huellas dactilares es el proceso más importante en los sistemas de autenticación biométricos basados en huella dactilar. De acuerdo a la puntuación obtenida en la correspondencia de huellas se autentica o no a una persona. Actualmente existen dos métodos, muy populares, de correspondencia dactilar, correlación y minucias. En este artículo, se evaluaron tres sistemas biométricos basados en huella dactilar: Neurotechnology Verifinger 6.0 SDK Extended, Innovatrics IDKit SDK y Griaule Fingerprint SDK 2007. La evaluación se llevo a cabo de acuerdo a las pruebas efectuadas en la Fingerprint Verification Competition (FVC). Se evaluó la influencia de la tolerancia de los grados de rotación en las huellas dactilares en las tasas de falsa correspondencia (FMR) y falsa no correspondencia (FNMR). Los resultados muestran que los valores de FMR incrementan a medida que la tolerancia de los grados de rotación también lo hace, en contraparte los valores de FNMR disminuyen. Los resultados mostraron que Verifinger obtuvo un buen desempeño en las pruebas de falsa no correspondencia, con un promedio de 7%, seguido de IDKit (entre 6.71% y 13.66%) y Fingerprint SDK (50%). Fingerprint SDK obtuvo un desempeño superior en las pruebas de falsa correspondencia con un promedio cercano al 0%, seguido por Verifinger (entre 7.62% y 9%) e IDKit (28%). Como resultado Verifinger tuvo el mejor desempeño general. Posteriormente se calcularon las funciones de regresión para predecir el comportamiento de las tasas de falsa correspondencia y falsa no correspondencia con diferentes valores de tolerancia y grados de rotación.

1. Introduction

Biometrics refers to methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits, such as voice, iris, retina, signature, face, fingerprints, palm print and DNA.

The employment of biometrics traits to identify persons guarantees accurate and reliable results. With this idea, biometric systems emerge as mechanisms for authentication, protection and access to information. At present, the most widely used biometric systems are fingerprint-based.
A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The uniqueness of a

fingerprint can be determined by the overall pattern of ridges and valleys as well as the local ridge anomalies [1].

A fundamental process in the fingerprint-based biometric system is the fingerprint matching. The matching algorithms must solve displacements and rotations of fingerprints since these factors affect the discriminate information.

Two fingerprint matching methods are the most popular: the correlation-based method and the minutiae-based method, being the last one the most frequently used [2, 3].

The evaluation of the fingerprint-based biometric system is carried out according to the errors that appear during its uses. Two fingerprint samples of the same finger are not exactly the same due to imperfections in the images acquired, physical changes in the fingerprint, environmental conditions and user interaction with the system [4].

During the fingerprint matching process, a score is generated as a result of the minutiae pairs that matched between fingerprints (in the case of the minutiae-based fingerprint matching methods). A threshold value is set to define the minimum score required to determinate if two fingerprints are similar. If the score is greater or equal than the threshold, then the fingerprints are similar, otherwise they are considered different.

It is therefore important to evaluate the matching algorithms before implementing them in real environment. Two indicators are considered as a measure of performance: the *false non-match rate* (FNMR), which is the probability of mistaking two fingerprints from one person for the fingerprints of two different persons; and the *false match rate* (FMR), which is the probability of mistaking fingerprints from two different persons for the fingerprints of one person [4].

Today, the test suite and fingerprint database designed by *Fingerprint Verification Competition* (FVC) is widely used [5-7]. The FVC fingerprint database contains a set of fingerprints which vary in quality, rotation and displacement. These factors make the fingerprint matching process of any matching algorithm difficult.

We selected three biometric systems, Neurotechnology Verifinger 6.0 Extended SDK, Innovatrics IDKit SDK and Griaule Fingerprint SDK 2007, to evaluate their performance. The selection of these matching algorithms was based on their multilanguage capacity, multiplatform, and compatibility with many commercial fingerprint readers.

Preliminary tests showed that fingerprint rotation degrees have an effect on the final results of FNMR and FMR. We decided to evaluate the rotation degrees for all the experiments and record the values of FNMR and FMR obtained. Matching algorithms allow comparing fingerprints with a rotation between 0 and 180 degrees. Usually, this parameter is not considered within the tests and the default value; in the majority of fingerprint-based biometric systems is 180° which allows fingerprint samples not to be restricted to intervals of rotation since it is often a reason for false rejections by biometric systems.

In Section 2, we will discuss briefly some matching algorithms and their performance. In Section 3, the experiments of this work will be detailed. Section 4 explains the results of the tests, Section 5 shows the regression functions calculated for Verifinger SDK, and finally, Section 6 presents the conclusions of this work.

2. Related work

With regard to the fingerprint matching methods, a great number of solutions have been proposed such as the correlation-based ones as well as the minutiae-based ones besides many hybrid models (correlation and minutiae). Hence the importance of measuring the behavior of FNMR and FMR of the proposed solutions against other existing ones.

The method proposed by Lindoso et al. [8] performs region selection to detect relevant information inside the fingerprint. In order to reduce the computational effort, a coarse alignment step is performed based in the cross-correlation of the orientation fields of fingerprints. The experimental results showed an *equal error rate* (EER) of 8%.
Another method proposed by Ouyang et al. [9] uses a local Fourier-Mellin Descriptor (FMD) and Phase-Only Correlation (POC) for partial

fingerprint verification. In the first step, the local FMDs and FMD Maps are calculated for template and query fingerprints in order to find the most likely FMD pair from fingerprints images. According to the pair, the fingerprints can be aligned; later, POC is used to find the similarity level between two FMDs. The experimental results showed an EER of 3.8%; if the proposed method is complemented with a minutiae-based technique, better results can be achieved.

In [10], a normalized cross-correlation technique that reduces the computational effort as well as the error rate better than the minutiae-based methods is proposed. The EER obtained is 2%.

Nandakumar and Jain [11] proposed a technique which employs local correlation around minutiae to improve the performance of a minutiae-based matcher. This method is compared with that of the 2D programming minutiae-based matcher proposed in [12]. The experimental results showed that the proposed method has a slightly inferior performance than the 2D programming matcher; however, if both merge, the EER is reduced (4.5%), improving the precision of the matching.

The minutiae-based methods are sensitive to rotation and displacements of fingerprints. Jain, Hong and Bolle [13] proposed a method that compensates these problems. This technique uses the ridge associated with minutia. With this information, the template and query fingerprints can be aligned.

Another minutiae-based method is proposed by Jiang and Yau [14], this method employs the local structure of minutiae and the global structures of fingerprint. The local structure of minutia is rotation and translation invariant; moreover, it can tolerate reasonable deformation. The global structure is used to align the fingerprint after minutiae matching in order to reduce the number of calculations required to align the fingerprints. The experimental results showed an EER of 0.45%.

Many times, the evaluation mechanisms of matching algorithms are not equal; this causes inconsistencies in the results when we want to perform comparisons among them. Therefore, the evaluation of the algorithms under the same criterion is necessary, considering a set of factors

that could significantly influence the behavior of these algorithms such as rotation, translation, source and quality of fingerprint images samples. We decided to evaluate a set of commercial fingerprint matching algorithms using the tests provided by the Fingerprint Verification Competition (FVC) considering the rotation degrees as factors that could influence negatively the behavior of these matching algorithms.

3. Test environment

The experiments are based on the tests from Fingerprint Verification Competition (FVC) [5]. Four indicators were measured: *false non-match rate* (FNMR), *false match rate* (FMR), *error equal rate*[1] (EER) and average matching time. As in the FVC, quality measuring mechanisms for fingerprints samples were not used.

The fingerprint dataset was taken from FVC 2002 [6], it consists of four groups with 800 fingerprints images each one. The 800 images are divided in 100 fingerprints from different fingers with 8 fingerprints samples from each one. The particularity of these groups is that each one of the fingerprints that integrate them were acquired using different types of fingerprint readers: the first and the second group were acquired using an optical fingerprint reader, the third group was acquired using a capacitive fingerprint reader, and the last one was generated with computer assistance, using the software SFinGE.

The FNMR test consists in the match between the samples of a same fingerprint. In the case of the FMR test, the first fingerprint sample of a person is matched against the first fingerprint sample of the other persons.

The fingerprint-based biometric systems evaluated are the following: Neurotechnology Verifinger 6.0 Extended SDK, Innovatrics IDKit SDK and Griaule Fingerprint SDK 2007. The matching algorithms

---

[1] The *Equal Error Rate* (EER) denotes the error rate at the threshold value (t) for which the false match rate and the false non-match rate are identical: FMR(t) = FNMR(t).

from these contestants are minutiae-based. The selection was based in 5 criteria:

• Multilanguage.
• Multiplatform.
• Support for multiple fingerprint readers.
• Technical documentation.
• Trial versions, without restrictions that could affect the performance of the biometric systems.

According to the documentation for each contestant, the threshold values (t) were established, having a minimum threshold value (t_{min}) and a maximum threshold value (t_{max}).

In the case of Verifinger SDK, its documentation did not specify a maximum threshold value so the first tests showed that the threshold values above 120 presented FMR values of 0. For this reason, we decided to evaluate Verifinger SDK with t_{max} = 120 with a constant interval of 6. In this way, each one of the algorithms has 21 threshold values for evaluation.

The false non-match and false match tests as well as operations to calculate FNMR, FMR, EER are detailed in [5, 6]. Before proceeding with the tests, the images were presented to each one of the matching algorithms in order to identify compatibility, reading and extracting minutiae issues; as a result of this action, no problem arose.

The configuration of the computer equipment where the tests were performed was as follows:

• PC Intel Pentium Core 2 Duo (T5250), 2 GB RAM and Microsoft Windows Vista.
• Programming language: Visual Basic .NET.

One of the factors that affect the performance of the matching algorithms is the fingerprint rotation. The tolerance to fingerprint rotation is a parameter that indicates the matching algorithm the maximum variation of rotation used to compare two fingerprints. It is estimated that with a lesser value of the rotation degree, the false non-match rate increases and vice versa. Otherwise on the false match tests, with a lesser value of the rotation degree, the false match rate decreases and vice versa.

The fingerprints of the collection did not show a rotation exceeding 35 degrees. We evaluated the algorithms in 4 rotation degrees values: 15°, 30°, 45° and 60°. The aim is to check if the rotation degree values increase; the algorithms become more or less discriminating during the tests.

Biometric System	Minimal threshold (t_{min})	Maximal threshold (t_{max})	Interval
Verifinger SDK	0	Unspecified	From 0 to 120 t_{max}, with a constant interval of 6.
Fingerprint SDK	0	200	10
IDKit SDK	0	20,000	1,000

Table 1. Threshold values for biometric systems.

4. Experimental results

The obtained results show that false non-match rates and false match rates are influenced slightly by rotation degrees. The values below are the average of the values of FMR and FNMR obtained in each one of the threshold intervals that we selected for each evaluated algorithm with different rotation degree values. The EER values are the average of the EER values obtained in each one of the tests for each rotation degree value. The average matching time is equal to the average time that the algorithm took to perform a single matching operation.

4.1 Fingerprint 2007 SDK

This algorithm presented very low values of FMR. Table 2 shows that false match rates are practically 0% in the four groups of fingerprints dataset. An exception appeared in the fourth group with at least one occurrence (false acceptance).

In Table 3, the first and second groups (optical fingerprint reader) showed a mean FNMR of 52.58% and 50.03%, respectively, the third group, 73.75%, and the fourth group, 65.24%. This means that Fingerprint 2007 SDK had a poor performance on fingerprints images acquired by capacitive fingerprint readers.

Degree	FMR			
	Group 1	Group 2	Group 3	Group 4
15°	0%	0%	0%	0%
30°	0%	0%	0%	0.02%
45°	0%	0%	0%	0.02%
60°	0%	0%	0%	0.02%
Mean	*0%*	*0%*	*0%*	*0.015%*

Table 2. FMR mean of Fingerprint SDK 2007.

Degree	FNMR			
	Group 1	Group 2	Group 3	Group 4
15°	60.31%	57.59%	77.63%	72.51%
30°	53.38%	50.87%	74.01%	63.17%
45°	48.39%	45.91%	71.73%	62.68%
60°	48.25%	45.75%	71.62%	62.59%
Mean	*52.58%*	*50.03%*	*73.75%*	*65.24%*

Table 3. FNMR mean of Fingerprint 2007 SDK.

Group	Average Matching Time (s)		EER
	FNMR	FMR	
1	0.00199829	0.00228186	2.73%
2	0.00220629	0.00249409	3.25%
3	0.0017678	0.00207081	9.14%
4	0.00198621	0.00219664	5.98%
Mean	*0.00198965*	*0.00226085*	**5.28%**

Table 4. EER and Average Matching Time of Fingerprint SDK.

With regard to the tolerance of the rotation degrees is observed that the values of FNMR decrease as the rotation increases. The following table shows the values of the EER and average matching time.

The matching algorithm took longer to verify the fingerprints of group 2. The EER of the group 3 presented a bigger value (9.14%) than the other ones did.

4.2 IDKit SDK

This software presented average values of FNMR lower than those shown by Fingerprint 2007 SDK; however, the obtained values of FMR were higher than the other matching algorithms (Table 5)

During the false matching tests, IDKit SDK showed a good performance. It is observed that the values of FMR increase slightly as the rotation degrees also does. The average values of FMR are group 1, 30.42%, group 2, 33.17%, group 3, 35.73%, and group 4, 28.81%. Again, group 3 obtained higher average values of FMR.

The average values of FNMR (Table 6) for group 1 is 8.49%, for group 2, 7.98%, for group 3, 13.66%, and for group 4, 6.71%. In the rotation degrees, it is observed that the values of FNMR decrease gradually as the degrees increase, except for group 2 and 4, particularly in the 60° angle of rotation, where the value of FNMR increases slightly. The third group showed average values of FNMR higher than the other algorithms.

Degree	FMR			
	Group 1	Group 2	Group 3	Group 4
15°	29.51%	32.54%	34.84%	25.51%
30°	30.57%	33.37%	35.89%	28.17%
45°	30.88%	33.53%	36.14%	30.20%
60°	30.73%	33.25%	36.03%	31.36%
Mean	*30.42%*	*33.17%*	*35.73%*	*28.81%*

Table 5. FMR mean of IDKit SDK.

Degree	FNMR			
	Group 1	Group 2	Group 3	Group 4
15°	15.05%	14.25%	19%	9.53%
30°	6.93%	6.95%	12.33%	5.76%
45°	5.98%	5.34%	11.68%	5.75%
60°	5.98%	5.36%	11.64%	5.79%
Mean	*8.49%*	*7.98%*	*13.66%*	*6.71%*

Table 6. FNMR mean of IDKit SDK.

Group	Average Matching Time (s)		EER
	FNMR	FMR	
1	0.0056812	0.06475546	4.70%
2	0.00756754	0.18248421	4.21%
3	0.00368285	0.27281647	6.59%
4	0.00548023	0.35482538	2.23%
Mean	0.00560296	0.21872038	4.44%

Table 7. EER and Average Matching Time of IDKit SDK.

The behavior of IDKit SDK regarding the source of fingerprints images is acceptable when they come from an optical fingerprint reader; however, for images coming from capacitive fingerprints readers, the performance of IDKit SDK is average. According to Table 7, the values of EER are better than Fingerprint 2007 SDK EER values, with a 4.44% mean of EER. However, the average matching time was superior in the four groups.

4.3 Verifinger 6.0 Extended SDK

The results obtained in the tests of this software showed a very good performance. The FNMR mean is lower than the other algorithms.

Degree	FMR			
	Group 1	Group 2	Group 3	Group 4
15°	7.99%	9.05%	7.10%	6.41%
30°	8.38%	8.96%	8.46%	7.63%
45°	8.53%	8.91%	8.87%	8.09%
60°	8.69%	8.93%	9.03%	8.35%
Mean	8.40%	8.96%	8.37%	7.62%

Table 8. FMR mean of Verifinger 6.0 Extended SDK.

Degree	FNMR			
	Group 1	Group 2	Group 3	Group 4
15°	14.52%	13.01%	15.09%	6.22%
30°	1.13%	1.22%	3.99%	2.99%
45°	1.04%	1.17%	3.88%	3.03%
60°	1.03%	1.17%	3.89%	3.04%
Mean	4.43%	4.14%	6.71%	3.82%

Table 9. FNMR mean of Verifinger 6.0 Extended SDK.

The FMR values (Table 8) increase as the rotation degrees increase too. The fourth group showed best results of FMR, followed by group 3, with 7.62% and 8.37%, respectively.

The mean FNMR (Table 9) is for group 1, 4.43%, for group 2, 4.14%, for group 3, 6.71%, and for group 4, 3.82%. The FNMR values for group 3 are higher than the ones for the other groups. The lowest FNMR values were registered in the fourth group, like IDKit SDK. According to the rotation degrees, in the first and second group, it is observed a slight decrease in the FNMR values as the rotation degrees increase. In the third and fourth group, this behavior is not present.

Verifinger showed the best average matching times in all groups (Table 10) in comparison to the other matching algorithms. The EER in all groups were slightly higher than the IDKit SDK EER values; nevertheless the EER value for the third group was the lowest one. The first and second group showed a mean value of EER higher than the fourth group, similar to IDKit SDK.

According to the experimental results, two groups showed the best and the worst performance among the algorithms: group 4 and 3, respectively. We wanted to know the behavior of FNMR and FMR for different threshold values not covered in the defined interval of threshold values, so we decided to calculate the regression functions that describe such behavior in these groups. Also we decided to calculate at 30° of rotation because is nearer to the maximum rotation value of the fingerprints samples in our database.

However, the fourth group belongs to fingerprints generated with computer assistance, in a real environment, the fingerprints basically are acquired by two types of fingerprints readers: optical and capacitive. So, we decided to change the fourth group for the second group, which showed, on average, the better performance of the optical fingerprints groups.

5. Regression functions

The regression functions of FNMR and FMR were calculated for different Verifinger threshold values. This decision was taken due to the fact that some threshold values were not evaluated in the tests and we wanted to know the behavior of the algorithm on those values.

The regression functions can be very helpful to obtain, for example, an equal error rate more precisely if we do not have all the threshold values where it can be evaluated a matching fingerprint algorithm.

Group	Average Matching Time (s)		EER
	FNMR	FMR	
1	0.00048986	0.00024349	5.99%
2	0.00072827	0.00043476	6.15%
3	0.00029223	0.0000745	4.85%
4	0.00044147	0.00013762	2.30%
Mean	0.00048796	0.00022259	4.82%

Table 10. EER and Average Matching Time of Verifinger 6.0 Extended SDK.

For example (Figure 1), the first calculated function that describes the behavior of FNMR in the second group (DB2) for the 30° angle or rotation was a lineal function:

$$FNMR_{2,30°}(x) = 0.00023x - 0.00176 \tag{1}$$

With a confidence of 97.77%, however, the next function calculated was a polynomial function (2) which had a confidence of 99.91%, higher than the confidence of the lineal function:

$$FNMR_{2,30°}(x) = 6 \times 10^{-13}x^6 - 2 \times 10^{-10}x^5 + 3 \times 10^{-8}x^4 - 2 \times 10^{-6}x^3 + 5 \times 10^{-5} x^2 - 0.0003x + 0.0007 \tag{2}$$

In Figure 2, the first calculated function was an exponential function (3):

$$FMR_{2,30°}(x) = 1.92620e^{-0.20766x} \tag{3}$$

with a confidence of 94.85%, a nearer approach is the polynomial function (4):

$$FMR_{2,30°}(x) = -0.00001x^4 + 0.00042x^3 - 0.0071x^2 - 0.01385x + 0.881 \tag{4}$$

with a confidence of 99.93% in the interval x = [0, 30] . For the interval x = (30, 120], the FMR value is 0. Another example is for the third group (DB3) for the 30° angle of rotation, the functions that models the behavior of FNMR (5) and FMR (6) are

$$FNMR_{3,30°}(x) = 6 \times 10^{-13} x^6 - 2 \times 10^{-10} x^5 + 3 \times 10^{-8}x^4 - 2 \times 10^{-6}x^3 + 6 \times 10^{-5} x^2 - 0.004x + 0.0062 \tag{5}$$

$$FMR_{3,30°}(x) = \begin{cases} -1\times10^{-9}x^6 + 2 \times 10^{-7}x^5 - 2\times10^{-5} x^4 + 0.005x^3 \\ \quad -0.0087x^2 + 0.0237x + 0.6514, x = [0,42] \\ \quad\quad 0, otherwise \end{cases} \tag{6}$$

With a confidence of 99.96% and 99.99%, respectively (Figure 3 and Figure 4).
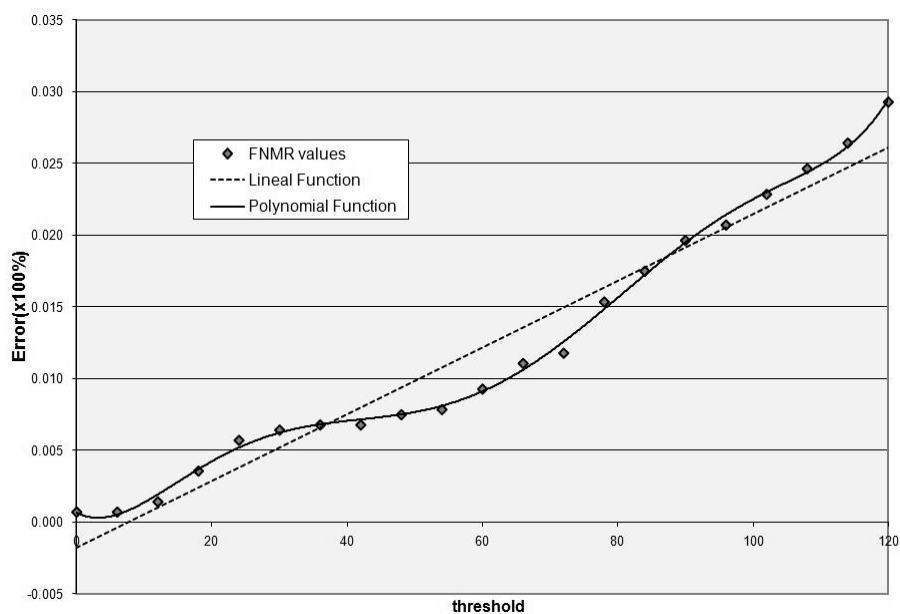
Figure 1. Regression functions of FNMR in the group 2 for 30º angle of rotation.
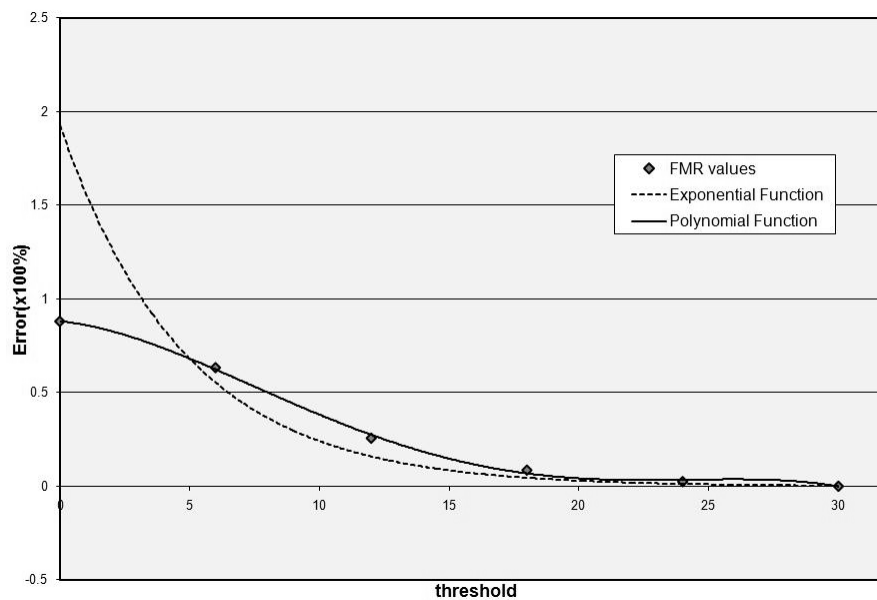

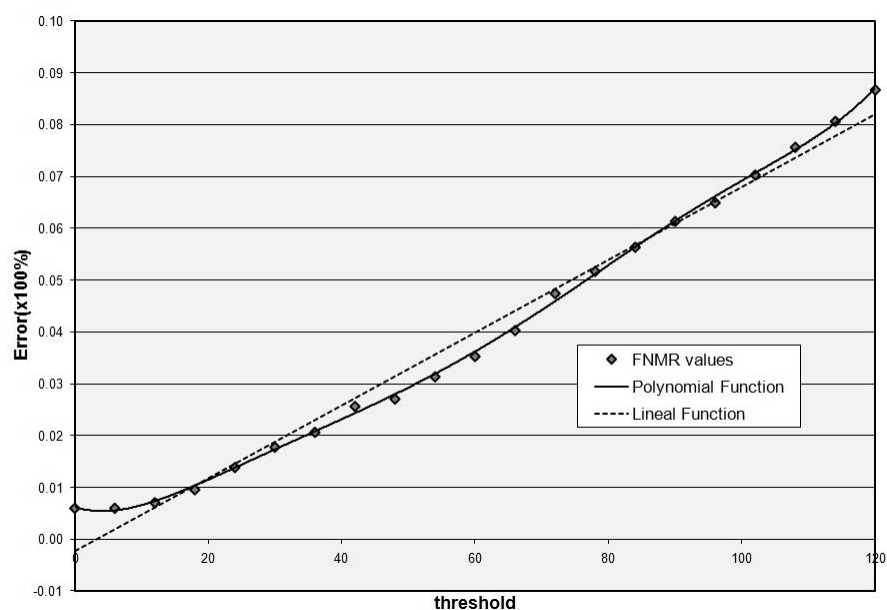Figure 2. Regression functions of FMR in the group 2 for 30º angle of rotation.

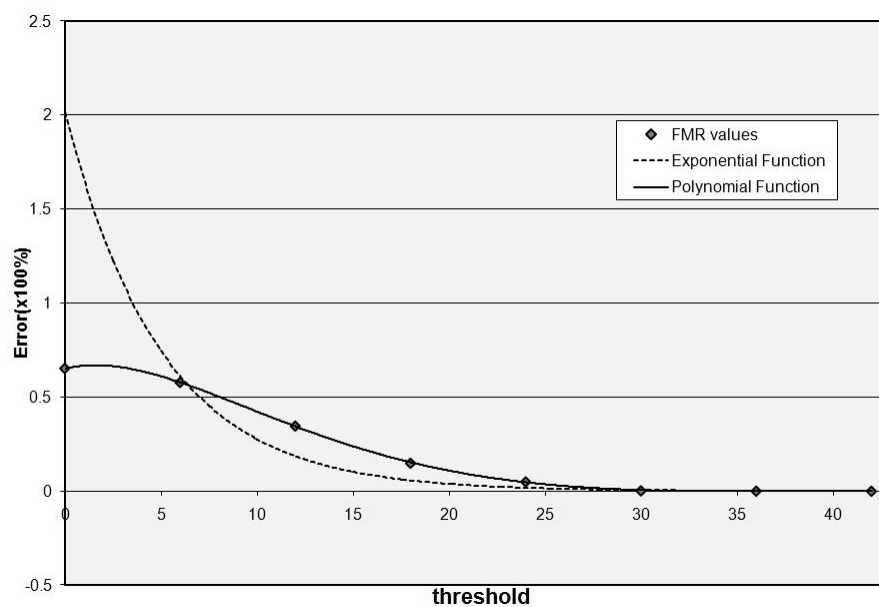Figure 3. Regression functions of FNMR in the group 3 for 30° angle of rotation.

Figure 4. Regression functions of FMR in the group 3 for 30° angle of rotation.

6. Conclusions and future work

The performance of the 3 fingerprint-based biometric system was measured according to the experiments from Fingerprint Verification Competition (FVC). We find that as the threshold values and rotation degrees increase, the FNMR values slightly decrease and FMR values increase. The experimental results favored Verifinger 6.0 Extended SDK in the FNMR test, which showed the best performance among the four fingerprints images groups with a mean below 7%, IDKit SDK showed FNMR mean values among 6.71% and 13.66%, followed by Fingerprint 2007 SDK with FNMR mean values above 50%.

However, Fingerprint 2007 SDK showed a very good performance in the FMR test, with a mean nearby 0% in the four groups, followed by Verifinger (among 7.62% and 9%) and IDKit with FNMR mean values above 28%.

In the Equal Error Rates, IDKit showed a better performance than the others (4.44%), followed by Verifinger (4.82%) and Fingerprint 2007 SDK (5.28%). Concerning the average matching time, in the 4 groups, Verifinger had the best average matching time in the FNMR and FMR tests with 4.87×10^{-4} s. y 2.22 x 10-4 s, respectively.

An important feature is that in the first and second group, fingerprints images acquired by an optical reader, had lower values for the error rates among the matching algorithms. In the third group, fingerprints images acquired by a capacitive reader, had the worst error rates values. In the fourth group, fingerprints images generated with computer assistance, the error rates values were lower than the error rate values reached in the first and the second groups for Verifinger SDK and IDKit SDK.

According to this, the SDK with a more stable and robust behavior was Verifinger 6.0 Extended SDK. So it was chosen to calculate the regression functions that model the behavior of FNMR and FMR in the second and third group (in these groups, the matching algorithms showed the best and the worst performance, respectively), the best functions that model the behavior of FNMR and FMR, were polynomial functions, with a confidence above 97%.

We recommend using small values of rotation degrees in order to diminish the probability of false acceptance. However, even with the performed experiments we cannot establish a specific relationship between the rotation degrees and the error rates so it is important to perform a greater number of tests between minutiae-based and correlation-based fingerprints matching algorithms.

References

[1] A. K. Jain, S. Pankanti, S. Prabhakar, and L. Hong, "Filterbank-based Fingerprint Matching," IEEE Transactions on Image Processing, vol. 9, pp. 846 - 859, May, 2000, 2000.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, 1th ed.: Springer, 2003.

[3] J. Woodward, N. M. Orlans, and P. T. Higgins, Biometrics: Identity Assurance in the Information Age, 1th ed.: McGraw-Hill, 2003.

[4] A. K. Jain, A. A. Ross, S. Prabhakar, and R. Bolle, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4 - 20, 30/1/2004, 2004.

[5] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint Verification Competition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, pp. 402 - 412, March, 2002, 2002.

[6] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second Fingerprint Verification Competition," in 16th International Conference on Pattern Recognition, 2002, 2002, pp. 811 - 814.

[7] D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition," in Proceedings of the First International Conference on Biometric Authentication, Hong Kong, 2004, pp. 1 - 7.

[8] A. Lindoso, L. Entrena, J. Liu-Jimenez, and E. S. Millan, "Increasing Security with Correlation-based Fingerprint Matching," in 41st Annual IEEE International Carnahan Conference on Security Technology, 2007, Ottawa, Ont., Canada, 2007, pp. 37 - 43.

[9] Z. Ouyang, J. Feng, F. Su, and A. Cai, "Fingerprint Matching with Rotation-Descriptor Texture Features," in The 18th International Conference on Pattern Recognition (ICPR'06), 2006, pp. 417 - 420.

[10] D. K. Karna, S. Agarwal, and S. Nikam, "Normalized Cross-correlation based Fingerprint Matching," in Fifth International Conference on Computer Graphics, Imaging and Visualization, 2008, pp. 229 - 232.

[11] K. Nandakumar and A. K. Jain, "Local Correlation-based Fingerprint Matching," Indian Conference on Computer Vision, Graphics and Image Processing, pp. 503 - 508, 18/12/2004, 2004.

[12] A. K. Jain, S. Prabhakar, and S. Chen, "Combining Multiple Matchers for a High Security Fingerprint Verification System," Pattern Recognition Letters, vol. 20, pp. 1371 - 1379, 1999.

[13] A. K. Jain, L. Hong, and R. Bolle, "On-line Fingerprint Verification," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, pp. 302 - 314, April, 1997, 1997.

[14] X. Jiang and W.-Y. Yau, "Fingerprint Minutiae Matching Based on the Local and Global Structures," in 15th International Conference on Pattern Recognition, 2000, Barcelona, Spain, 2000, pp. 1038 - 1041.

Authors´ Biographies

Jesús Arturo PÉREZ-DÍAZ

Dr. Perez-Diaz obtained his B.Sc. degree in computer science from the Universidad Autónoma de Aguascalientes in Mexico in 1995. He studied the program New Advances in Computer Science Systems and, during these years, he researched in mobile agents and published around 12 research papers in magazines and international conferences. He got his PhD degree in computer science from the Universidad de Oviedo in Spain in 2000. He researched in the field of mobile agents. He became a full associate member of the European founded research project AgentLink. During these years, he gave courses and made research in network and Internet security. Nowadays, he is a researcher and professor at the ITESM – Campus Cuernavaca, México and member of the National System of Researchers. His research field focuses in network security and wireless communications. He has been awarded by the CIGRE and by Intel for the development of innovative systems. Additionally, he is giving courses on wireless communications and network security in the postgraduate programs in the ITESM, also he has supervised master and PhD theses in the same field. He has given security courses in some European and South American Universities.

César Israel ARRONTE-LÓPEZ

He got his B.Sc. degree in computer systems from the Instituto Tecnológico Superior de Xalapa, Mexico in 2008. He obtained his master's degree in computer science in 2009 from the Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Cuernavaca. His areas of interest are biometrics and biometric authentication systems, home automation, networking and IT. He is currently developing multimedia entertainment systems and content management systems.