Performance Analysis of minutia-based fingerprint matching algorithms

[1]Mohamed Lahby, [2]Yassine Ismaili, [3]Abdelbaki Attioui and [4]Abderrahim Sekkaki
[1,3]Laboratory of Mathematics and Applications, university Hassan II, Ecole Normale Superieure (ENS) Casablanca, Morocco
[2,4]Laboratory of computer science and decision support, university Hassan II, Faculty of Sciences Ain Chock, Casablanca, Morocco
Emails: {medism@live.com, mlahby@gmail.com, silky.er@gmail.com, and a_sekkaki@fsac.ac.ma}

***Abstract*—The popular Biometric used to authenticate a person is Fingerprint. A minutia matching is widely used for fingerprint recognition. In this paper, we propose the performance analysis of some minutia-based fingerprint matching algorithms. For that, we present several algorithms for fingerprint matching, as well as the evaluation model used. All the algorithms are implemented in .NET Framework using the C# language. An experimental comparison among different matching algorithms is presented.**

***Index Terms*—biometrics, fingerprint matching, minutia, experimental result, evaluation model.**

I. Introduction

The types of information (features) that can be collected from a fingerprint impression can be classified in a hierarchy on three different levels: level 1 (global form of ridge pattern), level 2 (singularities and minutiae) and level 3 (pores, ridge contours, etc.).

In the literature, a large number of matching fingerprint algorithms have been proposed. According to [1] and [2], we can classify the different approaches of fingerprint matching into five large families: correlation-based, ridge feature-based, minutiae-based, level 3 based techniques and hybrid approaches. In this paper, we will focus on minutiae features and minutiae-based approaches.

These latters have been used in many commercial fingerprint matching systems. Based primarily on a point pattern matching model, these methods rely heavily on the accuracy of minutiae extraction and the detection of another features. According to a standard ISO/IEC 19794-2:2011 [3], the fundamental data elements used for minutiae-based representation of a fingerprint are: the type of the ridge (bifurcation, ridge ending), the coordinates (x,y) (in pixels), the direction θ (in radian).

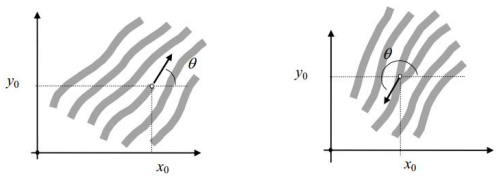

Fig. 1. Minutiae representation models

The figure 1, presents this information related to two types of minutiae most used: ridge ending (to the left), bifurcation (to the right). The minutiae-based approaches uses firstly local minutiae descriptors to coarsely align two fingerprints and then computes a global matching score based on minutiae correspondences [4], as shown in figure 2.

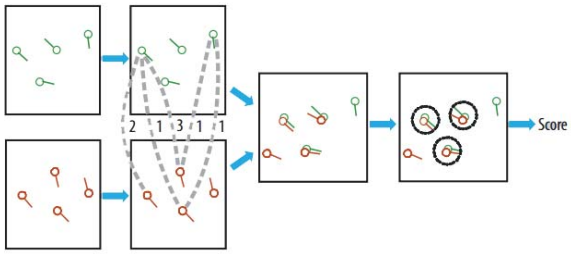

Fig. 2. Minutiae representation models

However, the majority of comparative approaches fingerprints are based on the comparison of minutiae. For this reason, the goal of this paper, is to develop effective methods for minutiae detection and extraction, in order to establish a reliable recognition system. The remainder of this paper is organized as follows. Section II presents an overview of fingerprint matching algorithms. Section III describes the databases used in this study, Section IV explores the evaluation model proposed for performance analysis of fingerprint matching algorithms. Section V includes the experimental results and discussion. Section VI concludes this paper.

II. A brief overview of fingerprint matching algorithms

Several minutiae-based fingerprint matching methods have been proposed and developed in the litterature. In [5], fingerprint minutia matching technique, which matches the fingerprint minutiae by using both the local and global structures of minutiae is proposed. The proposed minutiae matching scheme is suitable for an online processing due to its high processing speed. Experimental results show the performance of the proposed technique.

In [6], the authors have proposed a novel technique for fingerprint minutiae matching. This technique allows to connect minutiae using a delaunay triangulation and to analyze the relative position and orientation of each minutia with respect

978-1-5090-5781-8/16/$31.00 ©2016 IEEE

to its neighbors obtained by the triangle structure. Due to non-linear deformations, we admit a certain degree of triangle deformation. If rotations and translations are present, the triangle structure does not change consistently. The algorithm performance are evaluated on a public domain database.

In [7] the authors have proposed novel fingerprint matching algorithm, named M3gl. This algorithm contains three components: a new feature representation containing clockwise-arranged minutiae without a central minutia, a new similarity measure that shifts the triplets to find the best minutiae correspondence, and a global matching procedure that selects the alignment by maximizing the amount of global matching minutiae.

In [8] the authors have developed a novel fingerprint representation scheme that relies on describing the orientation field of the fingerprint pattern with respect to each minutia detail. This representation allows the derivation of a similarity function between minutiae that is used to identify corresponding features and evaluate the resemblance between two fingerprint impressions. The results show that, this novel fingerprint matching algorithm can achieve good performance on these data collections and that it outperforms other alternative approaches.

The authors [9] have introduced the Minutia Cylinder-Code (MCC) which is novel representation based on 3D data structures (called cylinders), built from minutiae distances and angles. The cylinders can be created starting from a subset of the mandatory features (minutiae position and direction) defined by standards like ISO/IEC 19794-2 (2005). Experimental results demonstrate that MCC is more accurate than wellknown minutiae-only local matching techniques. MCCis also very fast and suitable to be simply coded in hardware due to the bit-wise nature of the matching technique; this allows its porting on inexpensive secure platforms such as a smartcard or a system-on-a-chip.

SourceAFIS [10] is a fingerprint recognition/matching SDK (library), or more generally an Automated Fingerprint Identification System (AFIS). It essentially compares two fingerprints and decides whether they belong to the same person. It can quickly search a large database of registered fingerprints. It comes with an easy-to-use API (pure .NET and an experimental Java port) plus assorted applications and tools.

In [11] the authors have proposed a survey on fingerprint minutiae-based local matching for verification and identification. This study is devoted to review and categorize the vast number of fingerprint matching methods proposed in the specialized literature.

III. Biometric databases

In the literature review, variety of databases can be used in ordre to test the performance and behavior of the matching algorithms. In this study, we used three fingerprint databases, we presented their characteristics,their size and the average number of minutiae of the template and input fingerprints.

- FVC2000 DB1 B database [12]: contains 80 images from 10 individuals with eight samples from each user. The image size is 300x300 pixels and the resolution is 500 dpi, captured by a low-cost Optical Sensor "Secure Desktop Scanner";
- FVC2004 DB3 B database [13]: the image size is 300x480 pixels and the resolution is 512 dpi, captured by a thermal sweeping sensor "FingerChip FCD4B14CB";
- Neurotechnology Database [14]: the database consists of 51 different fingers with eight impressions per finger resulting in 408 images. The image size is 504x480 pixels and the resolution is 500 dpi. The fingerprint samples are scanned with an optical scanner Cross Match Verifier 300. The figure 3, shows One fingerprint example from each used database.

Fig. 3. Minutiae representation models

In additon, we used the feature extraction algorithms proposed by Ratha et al. [15]. These algorithms are used to extract orientation image, skeleton image and minutiae

IV. The evaluation model proposed for performance analysis fingerprint matching algorithms

In this section, we present the evaluation model proposed in [16]. This model will serve to evaluate fingerprint matching algorithms. The proposed evaluation model combines the multi criteria evaluation and criticality analysis and allows to assign a suitable weights for each evaluation parameters by multi criteria method. The operating principle of this evaluation process is based on seven steps:

1) Identification of the evaluation parameters: in our case, these parameters are the execution time and the similarity score. The execution time represents the comparison time in two fingerprints. The similarity score means the matching percentage between two fingerprints.
2) Construct the evaluation matrix: represents the matrix of the decision. It contains the evaluation of each matching algorithm Alg_i according to the evaluation parameter P_j. The decision matrix is expressed by the following equation:

$$EM = \begin{pmatrix} v_{11} & v_{12} & \dots & \dots & v_{1m} \\ v_{21} & v_{22} & \dots & \dots & v_{2m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \dots & \dots & v_{nm} \end{pmatrix} \quad (1)$$

Where v_{ij} is the measured value of fingerprint matching algorithm Alg_i with respect to the evaluation parameter P_j. The v_{ij} values are obtained from the simulation of matching algorithms.

3) Construct the normalized evaluation matrix: in order to controll the magnitude of evaluation parameters and to prevent that some of the evaluation parameters can dominate othoers, we calculate the normalized evaluation matrix by Max method normalization. Each element d_{ij} is computed as:
   - For benefit attribute, the normalized value of d_{ij} is computed as:
   $$d_{ij} = \frac{v_{ij}}{v_j^{max}} \quad (2)$$
   - For cost attribute, the normalized value of d_{ij} is computed as:
   $$d_{ij} = 1 - \frac{v_{ij}}{v_j^{max}} \quad (3)$$
4) Construct the criticality matrix: according to valuation scale defined in table I, we analyse the evaluation matrix obtained in second step. the criticality matrix c_{ij} is computed as:
   $$c_{ij} = k \quad (4)$$
   Where k is obtained from table I according to the value of d_{ij}

TABLE I
SCALE EVALUATION OF THE CRITICALITY MATRIX

Very low k=1	**Low k=3**	**Medium k=5**	**High k=7**	**Very hight k=9**
$d_{ij} > 80\%$ **of the max value**	$d_{ij} > 60\%$ **of the max value**	$d_{ij} > 40\%$ **of the max value**	$d_{ij} > 20\%$ **of the max value**	$d_{ij} <= 20\%$ **of the max value**

5) Construct the weighted criticality matrix: we apply multi criteria method to weigh each evaluation parameter, the weighted criticality matrix t_{ij} is computed as:
   $$t_{ij} = w_i * c_{ij} \quad where \sum_{i=1}^{m} w_i = 1 \quad (5)$$
6) Calculation of the criticality index: this index allows to measure the degree of importance of each matching algorithm Alg_i. The criticality index is calculated as:
   $$CI_i = 100 * (\sum_{j=1}^{m} t_{ij})/n \quad where\ i = 1, ..., n \quad (6)$$
   n is the maximum valuation level of all parameters.
7) Ranking: all matching algorithms can be ranked in descending order according to the criticality index CI_i.

V. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we analyze the results of the performances of six fingerprint matching algorithms namely:

- Algorithm proposed by "Jiang" and "You" (JY)
- Algorithm proposed by "Parziale" and "Niel" (PN)
- Algorithm proposed by "Miguel", "Medina", "Milton", "Gutierrez" and "Leopoldo" (M3GL)
- Algorithm proposed by "Tico" and "Kuosmanen" (TK)
- Algorithm "Minutia Cylinder-Code" (MCC) proposed by R. Cappelli et al.
- Algorithm proposed in the SDK (SourceAFIS)

We use databases DB1 B of FVC2000, DB3 B of FVC2004 competitions and Neurotechnology database. The performance evalution is focused on two parameters which are the measured by matching score and the execution time. The indicator time refers to the average matching time in milliseconds (ms). We carry out all the experiments on a laptop with an Intel Core i7-2620M processor (2.70 GHz) and 8 GB of RAM. Other indicators can be used also: EER, FMR100, FMR1000 and ZeroFMR. These performance indicators are used by fingerprint verification competitions [16].
We notice that, all algorithms are evaluated with their default parameters and we associate the same weight 0.5 for each evaluation parameter.

A. The experiment 1

This first experiment consists in comparing a fingerprint image with seven existing impressions of the same finger. This using the database DB1 B of FVC2000. An optical sensor with a low quality generates the images. We will focus on the average of the results provided in each comparison. Based on the previously mentioned evaluation model. Firstly, we will build the evaluation matrix containing the values obtained in the experiment as shown in table II.

TABLE II
EVALUATION MATRIX OF THE FIRST EXPERIMENT

Algorithms	**Matching Score** (%)	**Execution time** (ms)
SourceAFIS	18.92	11.28
MCC	8.87	4.85
TK	11.91	4.14
M3GL	31.96	0.1
PN	54.08	4.14
JY	57.03	0.87

Table III shows the scores and the criticality index of the all algorithms analyzed based on the first experiment. We notice that JY has the highest score, which means that this algorithm has the best performance than others.

TABLE III
EVALUATION ALGORITHMS USING DB1 B FVC2000

Algorithms	**Matching Score** (%)	**Execution time** (ms)	**Criticality index**
SourceAFIS	5	1	33.33
MCC	1	5	33.33
TK	3	7	55.56
M3GL	7	9	88.89
PN	9	7	88.89
JY	9	9	100.00

B. The experiment 2

This experiment consists in comparing a fingerprint image with seven existing impressions of the same finger by using the database DB3 B of FVC2004. The table IV shows the analytical results concerning the all algorithms.

TABLE IV
EVALUATION MATRIX OF THE SECOND EXPERIMENT

Algorithms	Matching Score (%)	Execution time (ms)
SourceAFIS	25.44	31.71
MCC	9.65	20.57
TK	2.56	35.14
M3GL	15.97	2.86
PN	38.55	52.14
JY	36.64	14.86

Table V shows the scores and the criticality index of the all algorithms analyzed, we notice that M3GL has the highest score, which means that this algorithm has the best performance than others algorithms.

TABLE V
EVALUATION ALGORITHMS USING DB3 B FVC2004

Algorithms	Matching Score (%)	Execution time (ms)	Criticality index
SourceAFIS	9	3	66.67
MCC	7	7	77.78
TK	1	3	22.22
M3GL	9	9	100.00
PN	9	1	55.56
JY	9	7	88.89

C. The experiment 3

In this experiment we analyse the seven existing impressions of the same finger by using using the Neurotechnology database. Images are captured using an optical sensor generating a good quality images.The table VI shows the analytical results concerning the all algorithms.

TABLE VI
EVALUATION MATRIX OF THE THIRD EXPERIMENT

Algorithms	Matching Score (%)	Execution time (ms)
SourceAFIS	36.02	33.00
MCC	10.77	26.00
TK	4.38	35.86
M3GL	27.48	3.28
PN	64.55	47.00
JY	60.09	17.00

Table VII shows the scores and the criticality index of the all algorithms analyzed based on the Neurotechnology database. We notice that M3GL has the highest score, which means that this algorithm has the best performance than others techniques.

TABLE VII
EVALUATION ALGORITHMS USING NEUROTECHNOLOGY DATABASE

Algorithms	Matching Score (%)	Execution time (ms)	Criticality index
SourceAFIS	9	3	66.67
MCC	5	5	55.56
TK	1	3	22.22
M3GL	9	9	100.00
PN	9	1	55.56
JY	9	7	88.89

VI. CONCLUSION

In this paper, we have presented a performance evaluation of minutiae-based fingerprint matching algorithms. According to the evaluation model adopted, the experiments show that the algorithm "JY" highly efficient in terms of speed and identification of different impressions of the same fingerprint with low quality images. As against the "M3GL" algorithm is efficient with medium and high quality images. These experimental results show also that M3GL require not much time and is more accurate than other algorithms based on minutiae triplets and other algorithms based on different representations.
We can explain this result by the rapidity of M3GL. In fact, it includes some optimizations to discard non-corresponding minutia triplets without comparing the whole representation.
In perspective, we intend to combine different strategies in order to obtain better results. Firstly, we will evaluate other minutiae-based matching algorithms. We will also confirm with adding other performance indicators. Finally, ws will investigate to do more experiments by evaluating images captured with other sensor types.

REFERENCES

[1] Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar *"Handbook of Fingerprint Recognition"*, Second Edition. Springer, 2009.

[2] Abhishek Rawat, *"A Hierarchical Fingerprint Matching System"*, Indian Institute of Technology Kanpur, 2009.

[3] ISO/IEC 19794-2:2011. *"Information technology – Biometric data interchange formats – Part 2:"*, Finger minutiae data, 2011.

[4] Anil K. Jain, Jianjiang Feng, and Karthik Nandakumar. *"Biometrics: Fingerprint matching"*, IEEE Comput. Soc. 2010.

[5] X. Jiang, W.Y. Yau. *"Fingerprint minutiae matching based on the local and global structures"*, International Conference on Pattern Recognition (ICPR),2000, pp. 6038-6041

[6] G. Parziale, A. Niel, *"A fingerprint matching using minutiae triangulation"*, In International Conference on Biometric Authentication (ICBA), Lecture Notes in Computer Science, vol. 3072, 2004, pp. 241-248.

[7] M.A. Medina-Prez, M. Garca-Borroto, A.E. Gutierrez-Rodrguez, L. Altamirano-Robles. *"Improving fingerprint verification using minutiae triplets, Sensors"*,12 (2012) 34183437.

[8] M. Tico, P. Kuosmanen. *"Fingerprint matching using an orientation-based minutia descriptor"*,In IEEE Trans. Pattern Anal. Mach. Intell. 25 (2003) 1009-1014

[9] R. Cappelli, M. Ferrara, D. Maltoni, *" Minutia cylinder-code: a new representation and matching technique for fingerprint recognition"*, IEEE Trans. 619 Pattern Anal. Mach. Intell. 32 (2010) 2128-2141

[10] Robert Vaan, *"SourceAFIS: Fingerprint recognition toolkit"*, Available: http://www.sourceafis.org/

[11] PERALTA, Daniel, GALAR, Mikel, TRIGUERO, Isaac, et al. *"A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation"*, Information Sciences, 2015, vol. 315, p. 67-87.

[12] *"FVC2000 - First International Competition for Fingerprint Verification Algorithms."*, Available: http://bias.csr.unibo.it/fvc2000/download.asp. [Accessed: 10-Jun-2016].

[13] *"FVC2004 - Third International Fingerprint Verification Competition"*, Available: http://bias.csr.unibo.it/fvc2004/download.asp. [Accessed: 10-Jun-2016].

[14] Neurotechnology,*"Sample fingerprint databases"*, Available: http://www.neurotechnology.com/download.html. [Accessed: 10-Jun-2016].

[15] Nalini K. Ratha, Shaoyun Chen, and Anil K. Jain. *"Adaptive flow orientation-based feature extraction in fingerprint images"*, Pattern Recognit. 2811 1657-1672, 1995.

[16] M. Lahby, C. Leghris. and A. Adib. *"An Enhanced Evaluation Model For Vertical Handover Algorithm In Heterogeneous Networks"*, In International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 3, No 2, pp.254-259, May 2012.