Anais do IX Congresso Brasileiro de Redes Neurais / Inteligência Computacional (IX CBRN)
Ouro Preto 25-28 de Outubro de 2009

FINGERPRINT MATCHING WITH A NEURAL NETWORK

Bernardo Sotto-Maior Peralva* Fernando Miranda Vieira Xavier* Augusto Santiago Cerqueira* David Sérgio Adães Gouvea* Marcos Fidelis Costa Campos*

*Electrical Engineering Post Graduation Program, Federal University of Juiz de Fora
University Campus, Juiz de Fora/MG, Brazil, 36036-030

Email: bernardo@labsel.ufjf.br, fernando@labsel.ufjf.br, augusto.santiago@ufjf.edu.br, dsergio.gouvea@ufjf.edu.br, marcos.fidelis@engenharia.ufjf.br

Abstract— This paper presents a novel method for fingerprint matching based on minutiae extraction that uses an artificial neural network as matching algorithm. The proposed method was implemented by software and its performance was evaluated and compared with another method, which is based on the spacial distance between the minutiae. The proposed method presented a good performance for the data set used in this work which is composed by selected images from the FVC2000 database.

Keywords— Pattern Recognition, Neural Networks, Fingerprint Identification, Minutiae.

1 Introduction

Biometric recognition refers to the use of distinctive physiological or behavioral characteristics (e.g., fingerprint, face, hand geometry, speech, iris, signature, etc), which are called biometric identifiers or simply biometrics, for the automatic recognition of a person (Maltoni et al., 2003).

The biometrics has grown significantly during the last years and several commercial systems are now available on the market, the majority of them based on the fingerprint. The main reasons for that are: the increase use of digital signal processing techniques, the growing capacity of the processors and memories and the security increase of the personal identification methods.

Despite the development during the last decades, the automatic fingerprint identification is still an important and challenging problem of pattern recognition, due to the complexity of the problem and the growing need for safety on personal identification (Maltoni et al., 2003). For example, varying skin and capture conditions often cause images of the same fingerprint to appear different.

The automatic fingerprint identification could be divided in three stages: (1) pre-processing; (2) parameter extraction; (3) fingerprint matching. The image enhancement is performed during the preprocessing envisaging the correction of the distortions and the enhancement of the image details that will be used as parameters by the matching algorithm. After the image pre-processing, the parameter extraction is performed envisaging the fingerprint matching that is performed on the third stage.

In this work, a multilayer neural network is used for fingerprint matching based on the minutiae extraction of the fingerprint image. A fingerprint image usually suffers severe distortions, including nonlinear ones. These distortions are corrected or attenuated by the pre-processing, but others do not. Therefore, the use of a neural network for fingerprint matching should be considered.

The proposed method was implemented by software and tested with images from a reference database (Maio et al., 2002). For performance comparison was also implemented a matching algorithm often used for fingerprint recognition based on the minutiae extraction (Maltoni et al., 2003), called here Standard method.

In the next section, the basic concepts of fingerprint recognition based on minutiae extraction is presented. Section 3 presents the proposed method for fingerprint matching. Section 4 shows the results for the proposed method and compares with the Standard method. Finally, in Section 5, the conclusions are derived.

2 Fingerprint Recognition Based on Minutiae Extraction

The fingerprint is basically formed by the configuration of the epidermal ridges and furrows. The ridges are the higher lines on the epidermal while the furrows the lower lines. An example of a fingerprint image can be seen in Figure 2(a). The local ridge characteristics is called *minute* details and the two most importante ridge characteristics, called minutiae, are the ridge termination and ridge bifurcation. A termination is defined as the ridge point where the ridge ends abruptly and a bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges.

Minutiae based methods are certainly the most well-known and widely used for fingerprint matching due to its strict analogy with the forensic

(a) (b)

Figura 1: An example of a fingerprint image (a) and the same image after the pre-processing described in Section 2.1 (b).

experts way to compare fingerprints and its acceptance as a proof of identity in the courts of law (Pankanti et al., 2002).

2.1 Pre-processing

The pre-processing for the minutiae based methods for fingerprint recognition envisages the enhancement of the difference between the ridges and furrows and the correction of the severe distortions that could occur during image acquisition.

Usually, the first step of the pre-processing is the image normalization in order to make the image contrast uniform. For that, the image is divided in blocks where the ridges could be considered approximately parallel straight lines. After the normalization, the orientation (Bazen and Gerez, 2002) and the frequency (Hong et al., 1998) maps should be obtained, showing the direction and the frequency of the ridges in each block, respectively. These maps are used for the image filtering (Hong et al., 1998) envisaging the image enhancement. After filtering, the image should be converted from gray-scale to black and white (binarization). Sometimes, the filtering already produces a binary output, and therefore the binarization is not needed. The binary images obtained are usually submitted to a thinning stage (Lam et al., 1992) which allows for the ridge line thickness to be reduced to one pixel. Finally, a simple image scan allows the detection of pixels that correspond to minutiae.

An example of a thinned fingerprint image (binary skeleton) after all procedures of the pre-processing can be seen in Figure 2(b). The original fingerprint image is the one in Figure 2(a).

In this work, the pre-processing followed the procedures described before and the details about the algorithms are described in (Castro, 2008).

2.2 Minutiae Extraction

A simple way to detect the minutiae is using the crossing number algorithm (Arcelli and Baja, 1984). Once a binary skeleton of a fingerprint image has been obtained, an image scan allows the minutiae detection and the pixels corresponding to minutiae are characterized by a crossing number different from 2. The crossing number $cn(\mathbf{p})$ of a pixel $\mathbf{p}$ in a binary image is defined as half the sum of the differences between pairs of adjacent pixels in the 8-neighborhood of $\mathbf{p}$ (Equation (1)),

$$cn(\mathbf{p}) = \frac{1}{2} \sum_{i=1..8} |val(\mathbf{p}_{imod8}) - val(\mathbf{p}_{i-1})|, \quad (1)$$

where $\mathbf{p}_0,\ \mathbf{p}_1,\ \ldots\ ,\ \mathbf{p}_7$ are the pixels belonging to an ordered sequence of pixels defining the 8-neighborhood of $\mathbf{p}$ and $val(\mathbf{p}) \in \{0, 1\}$ is the pixel value.

There are several ways to perform the minutiae detection, but in this work, the crossing number were used for minutiae extraction.

2.3 Fingerprint Matching

Let $\mathbf{T}$ and $\mathbf{I}$ be the representation of the template and input fingerprint, respectively. Unlike in correlation-based techniques, where the fingerprint coincides with the fingerprint image, here the representation is a feature vector whose elements are the minutiae. Each minutia may be described by a number of attributes, including its location in the fingerprint image, orientation, type (termination and bifurcation), and so on. Most minutiae matching algorithms consider each minutiae as a triplet $\mathbf{m} = \{x, y, \theta\}$ that indicates x, y the minutia location coordination and θ the minutia angle (Equation (2)).

$$\begin{array}{l} \mathbf{T} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_m\}, \\ \mathbf{m}_i = \{x_i, y_i, \theta_i\}, \;\; i = 1, ..., m, \\ \mathbf{I} = \{\mathbf{m'}_1, \mathbf{m'}_2, \ldots, \mathbf{m'}_n\}, \\ \mathbf{m'}_j = \left\{x'_j, y'_j, \theta'_j\right\}, \;\; j = 1, ..., n, \end{array} \quad (2)$$

where m and n denote the number of minutiae in T and I, respectively.

A minutia $\mathbf{m'}_j$ in $\mathbf{I}$ and a minutia $\mathbf{m}_i$ in $\mathbf{T}$ are considered "matched"if the *spatial distance* (sd) between them is smaller than a given tolerance r_0 and if the *direction difference* (dd) between them is smaller than an angular tolerance θ_0, as described in (3) and (5), respectively.

$$sd(\mathbf{m'}_j, \mathbf{m}_i) = \sqrt{(x'_j - x_i)^2 + (y'_j - y_i)^2} \leq r_0 \quad (3)$$

$$dd(\mathbf{m'}_j, \mathbf{m}_i) = min(|\theta'_j - \theta_i|, \quad 360° - |\theta'_j - \theta_i|) \leq \theta_0 \tag{4}$$

The alignment of the two fingerprints is a mandatory step to maximize the number of matching minutiae. The correct alignment of two fingerprints requires *displacement* (in x and y) and rotation (θ) to be recovered and, likely, can involve others transformations because the fingerprint can be affected by severe distortions (Maltoni et al., 2003).

In this work, only the *spatial distances* between the minutiae are used for comparison. This method of fingerprint matching is called here Standard method.

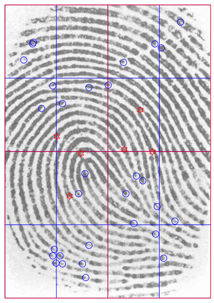
3 Proposed Method for Fingerprint Matching

In this work, a neural network is used to perform the fingerprint matching aiming at the correction of the distortions which are not completely removed at the image pre-processing stage. In this way, after the system design step, the features extracted from the pair of fingerprint images should be presented to the neural network as its input parameters. The neural network output informs whether this pair matches or not.

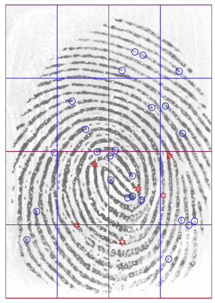
3.1 Feature Extraction for the Neural Network Matching

The minutiae vector can not be directly presented to a neural network due to the variable number of minutiae extracted from image to image. Thus, in order to extract the same number of parameters for any collected fingerprint, the minutiae vector is divided in 16 sectors. Figure 2 illustrates two fingerprint images from different fingers divided in 16 sectors (shown as the rectangles in the figure), as well as the detected minutiae (circles). To avoid a large number of false minutiae detected on the superior and inferior parts of the fingerprint due to the distortions occurred during the image acquisition, only the information contained in the eight central sectors is used on further processing.

In order to represent the minutiae information concerning each sector, the mean position is estimated according to the Equation (5), where x_m and y_m correspond to the mean value estimation of the x y coordinates of the minutiae, N to the number of minutiae and x_n and y_n refer to the coordinates of each single minutia.



(a)



(b)

Figura 2: Image division in Sectors and the detected minutiae for the fingerprint pair selected for matching.

$$x_m = \frac{\sum_{n=1}^{N} x_n}{N}, \quad y_m = \frac{\sum_{n=1}^{N} y_n}{N} \tag{5}$$

From the mean coordinates of the minutiae of each sector (x_m and y_m), the spatial distance sd of the fingerprint pair in comparison is calculated through the use of the Equation (3).

The information related to the number of minutiae contained in each sector is also used as the input information to the neural network, as shown in the Equation 6, where N_1 and N_2 are the number of minutiae of the first and the second fingerprint, respectively. The α and β are arbitrary constants greater than 1.

$$e_i = sd\frac{\alpha^{|N_1 - N_2|}}{\beta^{(N_1+N_2)/2}} \tag{6}$$

Finally, the Vector $\mathbf{V_{NN}}$ (7) is derived and used as the input of the neural network. The element e_i corresponds to the compressed information belonging to the each sector of the fingerprint pair. Accordingly (6), 16 parameters are extracted from the fingerprint pair, 8 for the termination and 8 for the bifurcation of the eight sectors.The parameters are sorted in valve order to be presented to the neural network.

$$V_{NN} = [e_1 \ e_2 \ \dots \ e_{16}] \tag{7}$$

3.2 The Fingerprint Matching

Once the parameters are extracted from the fingerprint pair, an artificial feedforward multi-layer neural network is used to perform the fingerprint matching.

3.2.1 Training Methodology

The proposed method makes use of a supervised training algorithm, therefore, the first step is to generate from a known fingerprint database, several pairs of fingerprints. For each pair is known whether they come from the same fingerprint or not.

For each fingerprint pair the input parameters of the neural network should be extracted as described above. These several input vectors of the neural network are divided in two sets, the training and test sets. The training set is used for the synaptic weights update, while the test set is only used for performance evaluation. It is worth mentioning that for an efficient classification the two sets must contain similar numbers of equal and different fingerprints.

In order to improve the generalization of the neural network, the criteria to stop the training should be the efficiency on the test set, avoiding overtraining.

3.2.2 Application on Fingerprint Identification

In a fingerprint identification problem, a collected fingerprint is compared with the ones into the database, searching for a matching and, therefore, searching for a personal identification.

The proposed neural network matching method can be used in a fingerprint identification problem. In Section 4, the performance of the proposed method is evaluated envisaging its application into a fingerprint identification problem. For this, the trained neural network should be used for matching each fingerprint pair formed by the collected fingerprint with the database fingerprints.

4 Results

In this section, the proposed method is implemented by software and its performance is evaluated in a fingerprint identification problem. A comparison with the Standard method is also performed.

4.1 Database

To verify the efficiency of the proposed method in a fingerprint identification problem a reference database is used (Maio et al., 2002). This database were used on the Fingerprint Verification Competition of year 2000 (FVC2000) and is available electronically. From this database, 369 pairs of fingerprints were selected, where 186 correspond to pairs of images from the same fingerprint and 183 correspond to pairs of images from different fingerprints. From the selected fingerprints, 152 were used as training set, 104 as the test set and 113 as a validation set. The training and the test sets are used during the system design and the validation set is used to verify the system performance.

4.2 Neural Network Design

The proposed method faces the matching problem as a classification problem with two classes, one class of matched fingerprint pairs and another class of non-matched fingerprint pairs. A multilayer feed forward neural network is used for classification with the resilient back-propagation as a training algorithm.

The neural network input vector has only 16 parameters as presented in Section 3.1. The neural network activation function is the hyperbolic tangent for all neurons. The number of layers as well as the number of neurons in each layer was defined by optimizing several times the neural network with different topologies, choosing the one with best performance. The configuration which fits best the application has two hidden layers with 20 and 10 neurons respectively, and a single neuron at the output layer.

The fingerprint pair at the neural network input is considered matched if the resulted neural network output is non-negative, otherwise, the fingerprint pair is considered non-matched.

4.3 Performance Evaluation

The performance evaluation of the proposed method for fingerprint identification is presented in terms of its False Non-Match Rate (FNMR) and False Match Rate (FMR). The FNMR is the probability of falsely non-matching and the FMR the probability of a false matching.

As mentioned in the Section 3, the efficiency of the neural network over the test set is used to stop the training. Table 1 shows the best results for the training and test data sets in terms of its FNMR and FMR. For comparison, it is also shown the results for the Standard method, which uses both training and test data sets for design.

Once the neural network achieves its best performance during the learning phase, the neural network could be applied for fingerprint identification through the use of the validation data set. During the validation, the neural network parameters are fixed and the data are presented to the neural network for classification. The results are shown in Table 2 and for comparison is also shown the results for the Standard method.

Tabela 1: False Non-Match and False Match Rates for the Training and Test Sets.

Method	Data Set		Efficiency
	Training	Test	
Proposed	0 %	1.9 %	FMR
	0 %	0 %	FNMR
Standard	1.5 %		FMR
	0 %		FNMR

Tabela 2: False Non-Match and False Match Rates for the Validation Set.

Method	Validation	
	FMR	FNMR
Proposed	1.8 %	1.7 %
Standard	3.6 %	0 %

5 Conclusions

In this paper, a neural network matching method for fingerprints based on minutiae extraction was presented. The application of neural networks for fingerprint matching is still not well explored, but this paper indicates that it is a good approach for fingerprint matching.

The advantage of the neural network over the methods based on the minutiae *spacial distances* and *direction distances* is the ability of the neural network to cope nonlinear distortions that are not removed during the pre-processing.

The proposed method of fingerprint matching was evaluated in a fingerprint identification problem and compared with a matching algorithm based on the *spacial distances* between the minutiae. The results showed that the proposed method achieved similar results for the data set used in this work.

It is important to stress that this paper presents a initial approach for the neural network fingerprint matching. There are, still, a lot of work to be done on the parameters extraction for the neural network to make the method more robust in terms of image distortions not corrected by the pre-processing.

Acknowledgements

We are thankful to the Federal University of Juiz de Fora, CNPq, CAPES and FAPEMIG for the financial support to this work. Also, we would like to thank our colleague M.Sc. Thiago da Silva Castro, without him this work could not be done.

References

Arcelli, C. and Baja, G. S. D. (1984). A width independent fast thinning algorithm, *IEEE Transactions on Information Forensics and Security* **4**(7): 463–474.

Bazen, A. M. and Gerez, S. H. (2002). Systematic methods for the computation of direction fields and singular points of fingerprints, *IEEE Trans. on Pattern Analysis and Machine Intelligence* **24**(7): 905–919.

Castro, T. S. (2008). *Fingerprint Identification Based on Minutiae Extraction*, Master thesis, Federal University of Juiz de Fora. Brazil.

Hong, L., Wan, Y. and Jain, A. K. (1998). Fingerprint image enhancement: Algorithms and performance evaluation, *IEEE Trans. on Pattern Analysis and Machine Intelligence* **20**(8): 777–789.

Lam, L., Lee, S. W. and Suen, C. Y. (1992). Thinning methodologies: A comprehensive survey, *IEEE Trans. on Pattern Analysis and Machine Intelligence* **14**(9): 869–885.

Maio, D., Maltoni, D., Cappeli, R., Wayman, J. L. and Jain, A. K. (2002). FVC2000: Fingerprint Verification Competition, *IEEE Trans. on Pattern Analysis and Machine Intelligence* **24**(3): 402–412.

Maltoni, D., Maio, D., Jain, A. K. and Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*, Springer.

Pankanti, S., Prabhakar, S. and Jain, A. K. (2002). On the individuality of fingerprints, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **24**(8): 1010–1025.