FINGERPRINT MATCHING APPROACH USING A NOVEL METRIC

Tudor BARBU[1]

În această lucrare propunem o tehnică de recunoaştere a amprentelor digitale. Abordarea noastră presupune efectuarea unui proces de potrivire a minuțiilor. Mai întâi este efectuată o operație de extragere a trăsăturilor, bazată pe minuțiile amprentei. O procedură de clasificare supervizată este aplicată apoi vectorilor de trăsături obținuți. Am construit o metrică potrivită pentru aceşti vectori, care este utilizată în procesul lor de clasificare. Această metrică specială reprezintă prinicipala contribuție a lucrării. Alte contribuții sunt: modelul propus pentru vectorul de trăsături,clasificatorul de distanță medie minimală şi metoda de verificare bazată pe prag.

We propose a supervised fingerprint recognition technique in this paper. Our approach performs a minutiae matching process. A minutiae based fingerprint feature extraction is performed first. Then, a supervised classification procedure is applied on the resulted fingerprint feature vectors. We create an appropriate metric for these feature vectors, to be used in the classification process. This special metric represents the main contribution of this work. Other contributions are: the proposed feature vector model, the minimum mean distance based classifier and the threshold based verification approach.

Keywords: fingerprint recognition, minutiae matching, feature vector, novel metric, supervised classification, fingerprint identification, verification.

1. Introduction

Fingerprints represent one of the most known forms of biometrics used to authentify human persons. Because of their uniqueness and consistency over time, fingerprints have been used for person recognition for over a century [1].

Fingerprint recognition represents the computerized automated process of determining the identity of an individual using the characteristics of his fingerprints. Obviously, a fingerprint recognition system is a biometric authentication system [1]. Therefore, it performs two main processes: *identification* and *verification*.

[1] CP II, Institute of Computer Science, Romanian Academy, Iassy, Romania, e-mail: tudbar@iit.tuiasi.ro

Fingerprint identification associates each input fingerprint with a registered user of the system. It consists of two essential operations: fingerprint feature extraction and feature vector classification.

Fingerprint verification represents the task of validating the associated identity of a fingerprint. Verification algorithms usually use proper threshold values.

The main application area of fingerprint recognition systems is law enforcement. Another important application field of fingerprint authentication is access control to various services, numerous security systems being based on fingerprints [2].

The fingerprint recognition techniques are divided into two main categories: *minutiae-based* [3,4] and *pattern-based* approaches [5]. As one knows, a human fingerprint is composed of *ridges* and *valleys*, situated on the surface of the finger. The patterns represent aggregate characteristics of ridges and *minutia points* [1]. We will approach minutiae-based fingerprint recognition only in this paper.

Most modern fingerprint matching technologies are based on minutiae matching [3]. Minutia points are unique features found within the patterns. The idea of the matching is if one can find enough minutiae in one image that have corresponding minutiae in another image, then the images are most likely from the same fingerprint.

There are various types of minutia details such as: ridge endings, bifurcations, short ridges, dots, crossovers, spurs and islands [2]. The most important fingerprint points are the ridge endings, short ridges and bifurcations. The most commonly used minutiae in current fingerprint recognition technologies are ridge endings and bifurcations. We also use ridge endings and bifurcations in our matching approach.

A minutiae-based fingerprint recognition approach consists of two parts, which are: *minutiae detection* and *minutiae matching*. We do not provide any new solutions for minutia point detection [6,7], focusing on minutiae matching instead [3,8]. Thus we propose a fingerprint feature extraction approach, the obtained minutiae-based featuring model being described in the next section.

The distance between resulted feature vectors is measured using a novel metric introduced in the third section. This special metric, representing the main contribution of this paper, is used in the fingerprint classification process.

We propose a supervised classification technique, based on the minimum average distance between feature vectors and presented in the fourth section. A fingerprint verification method is proposed in the same section. In the fifth section are mentioned some experiments. This paper ends with a conclusions section and references.

2. Minutiae-based fingerprint feature extraction model

As we have mentioned in introduction, a minutiae detection process has to be performed before fingerprint matching. There are many available minutiae extraction algorithms. Most of them extract the fingerprint ridges by performing binarization and thinning of fingerprint images [3,6].

However, there exist some direct minutiae extraction techniques. They identify the fingerprint minutia points by following the ridge line in the grayscale image of the fingerprint [7].

We consider a binarization-based approach to this task. The minutiae detection procedure performs three main operations: fingerprint binarization, skeletonization and minutia point identification.

The first operation means performing a conversion of the grayscale image of the analyzed fingerprint into a binary format. A threshold-based process can be applied in this case. Black areas from the resulted binary image represent the ridges.

Next operation, the skeletonization, produces the *morphological skeleton* of the binary image of the fingerprint [9]. Skeletonization task is performed using a *thining* algorithm. Image thinning represents a morphological process that is similar to erosion and opening. It produces very thin ridges, having a width of one pixel [9].

The most popular thinning algorithms are medial axis method, contour generation method, local thickness based thinning approach, sequential and parallel thinning [6,10]. A well-known parallel thinning algorithm is that developed by T. Zhang and C. Suen in 1984 [10].

The thinned ridges facilitate the fingerprint minutiae detection task. We consider *8 – neighborhoods* of black pixels in this identification process. For each black pixel (having 0 value) of the skeleton, one determines if it represents either a minutia point or an ordinary pixel.

The detection algorithm counts the number of neighbours of the current black pixel. There could be three possible situations. If the pixel has only one neighbou, then it represents a **ridge ending.** If the pixel has at least 3 neighbours, then it represents a **bifurcation.** If the pixel has 2 neighbours, then it is an intermediary pixel.

We performed many minutiae detection experiments using this described approach. Such a minutia point identification example is presented in Fig. 1. One can observe a grayscale fingerprint that is converted into binary form, then a skeletonization process is applied and finally, the minutiae details are extracted from it.

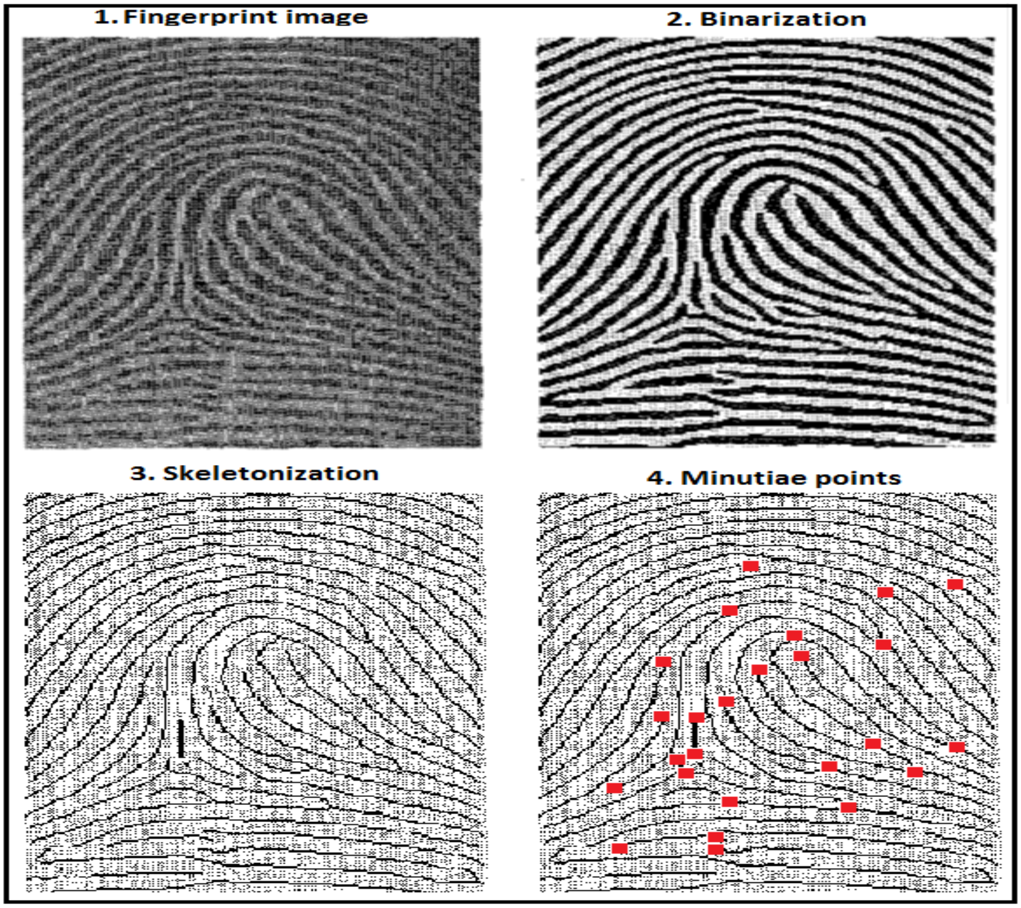

Fig. 1. Minutiae detection example

In our approach the feature vector of a fingerprint image is composed of the feature vectors corresponding to the detected minutiae [8]. So, if F represents a fingerprint image, then $\left\{M_1^F,...,M_{m(F)}^F\right\}$ is the sequence of the minutia points identified in F. Obviously, $m(F)$ is the number of these characteristics corresponding to F. The fingerprint feature extraction process can be modeled as follows:

$$V(F)=\left[V(M_1^F),...,V(M_{m(F)}^F)\right] \tag{1}$$

where $V(M_i^F)$ represents the feature vector of M_i^F, $i\in\left[1,m(F)\right]$. Each of these vectors has to contain the essential information related to the corresponding minutia: its *type* (ridge ending, bifurcation), its *position* (provided by coordinates) and its *orientation,* representing the angle of the minutia tangent and orizontal axis [3,8]. Therefore, the feature vector of a fingerprint minutia is expressed in the following form:

$$V(M_i^F) = \left[Type_i^F, x_i^F, y_i^F, \theta_i^F\right] \tag{2}$$

where $Type_i^F$ represents the minutia type of M_i^F, x_i^F and y_i^F are its coordinates, and θ_i^F represents the orientation of M_i^F. These measures of a minutia, which compose the feature vector, are represented in Fig. 2.

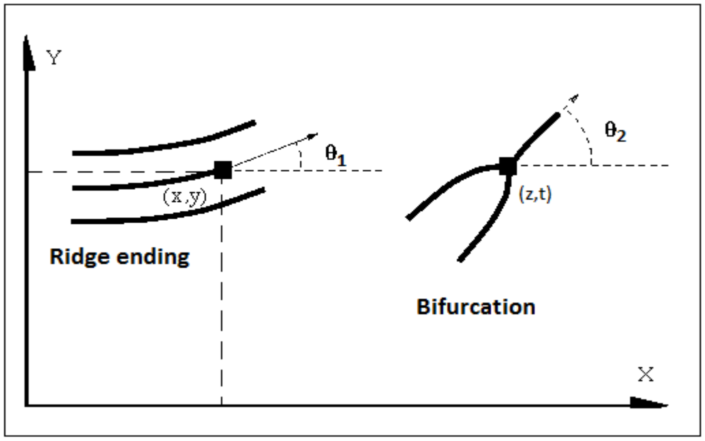

Fig. 2. Main minutia measures

From relations (1) and (2) we obtain the final form of the feature vector of fingerprint *F*:

$$V(F) = \left[\left(Type_1^F, x_1^F, y_1^F, \theta_1^F\right), \ldots, \left(Type_{m(F)}^F, x_{m(F)}^F, y_{m(F)}^F, \theta_{m(F)}^F\right)\right] \tag{3}$$

The components M_i^F are positionated in the sequence corresponding to *F* on the basis of their coordinates. They are aligned from left to right and from top to the bottom, therefore we have:

$$\begin{cases} x_1^F \leq \ldots \leq x_i^F \leq \ldots. \leq x_{m(F)}^F \\ x_i^F = x_{i+1}^F \Rightarrow y_i^F < y_{i+1}^F \end{cases} \tag{4}$$

The fingerprint feature vectors computed by (3) have to be classified using a proper metric. In the next section we propose a novel special metric that is able to measure the distance between these structures.

3. A special distance function for fingerprint feature vectors

The feature vectors defined by relation (3) represent structures having variable dimensions, depending on the number of minutiae detected in each fingerprint. Therefore, the distances between them cannot be computed using well-known metrics such as Euclidian distance.

For this reason we develop a proper metric, that is able to compare different sized feature vectors and it is related to the number of minutiae matchings. For simplicity, let us consider the general case of two feature vectors, $v = [v_1,...,v_n]$ and $w = [w_1,...,w_k]$, where the components v_i and w_j represent vectors having the same length. The metric computing the distance between *v* and *w* is defined as:

$$d(v,w) = \frac{n+k}{2} - p(v,w) \tag{5}$$

where *p*(*v*,*w*) computes the number of de matchings between *v* and *w*, therefore having the form :

$$p(v,w) = card\ \left(\left\{i \in [1, \min(n,k)] \middle| v_i = w_i\right\}\right) \tag{6}$$

The function *d*, expressed by (5), satisfies all the defining properties of a distance. Let us demonstrate each of them.

1. **Non-negativity:**

$$p(v,w) \le \min(n,k) \Rightarrow p(v,w) \le \frac{n+k}{2} \Rightarrow \frac{n+k}{2} - p(v,w) = d(v,w) \ge 0 \tag{7}$$

2. **Leibniz rule:** one proves the equivalence $d(v,w) = 0 \Leftrightarrow v = w$. Its second part is solved as follows:

$$v = w \Rightarrow p(v,w) = p(v,v) = n \Rightarrow d(v,w) = d(v,v) = \frac{n+n}{2} - n = 0 \tag{8}$$

For the first part of the rule, we have:

$$d(v,w) = 0 \Rightarrow \frac{n+k}{2} = p(v,w) \le \min(n,k) \Rightarrow n + k \le 2 \cdot \min(n,k) \tag{9}$$

but $n + k \ge 2 \cdot \min(n,k)$, therefore $n + k = 2 \cdot \min(n,k) \Rightarrow n = k. \Rightarrow p(v,w) = n$. This means the two vectors have the same length, that is equal to number of matchings, therefore *v* = *w*.

3. **Simmetry:** From *p*(*v*,*w*) = *p*(*w*,*v*) it results, obviously, that *d*(*v*,*w*) = *d*(*w*,*v*).

4. **Subadditivity (triangle inequality):**

We consider a third structure of this type, $u = [u_1,...,u_t]$, and prove that $d(u,v) \le d(u,w) + d(v,w), \forall u,v,w$. We introduce $p_w(u,v)$, representing the number of matchings between *u* and *v* but cannot be found in *w*. Therefore, we have:

$$p(u,v) = p_w(u,v) + p(u,v,w) \tag{10}$$

where

$$p_w(u,v) = card\left(\left\{i \in \left[1, \min(t,n)\right] \middle| u_i = v_i \neq w_i\right\}\right) \tag{11}$$

and *p*(*u*,*v*,*w*) return the number of matchings between all the three structures, being expressed as:

$$p(u,v,w) = card\left(\left\{i \in \left[1, \min(t,n,k)\right] \middle| u_i = v_i = w_i\right\}\right) \tag{12}$$

From (10) it results that $d(u,v) = \frac{n+t}{2} - p_w(u,v) - p(u,v,w)$, while $d(u,w) + d(v,w) = \frac{n+t}{2} + k - 2 \cdot p(u,v,w) - p_v(u,w) - p_u(v,w)$. Therefore, the triangle inequality becomes equivalent to this inequality :

$$k - p_v(u,w) - p_u(v,w) - p(u,v,w) \geq -p_w(u,v) \tag{13}$$

As one knows, *k* represents the number of al components of *w*. Therefore, it results :

$$k \geq p_v(u,w) + p_u(v,w) + p(u,v,w) \tag{14}$$

which means that $k - p_v(u,w) - p_u(v,w) - p(u,v,w) \geq 0 \geq -p_w(u,v)$, therefore relation (13) is validated and so is the triangle inequality : $d(u,v) \leq d(u,w) + d(v,w)$

Metric *d* is then applied for fingerprint feature vectors given by (3). If F_1 and F_2 are two fingerprint the distance function computed by (5) becomes:

$$d(V(F_1),V(F_2)) = \frac{m(F_1) + m(F_2)}{2} - p(V(F_1),V(F_2)) \tag{15}$$

We consider that a matching between minutia points means a perfect equality between their types, but an approximate equality between the corresponding coordinates and angles. Therefore, the number of matchings is computed as :

$$p(V(F_1),V(F_2)) = card\left\{i \leq \min\left(m(F_1),m(F_2)\right) \middle| Type_i^{F_1} = Type_i^{F_2}, x_i^{F_1} \cong x_i^{F_2}, y_i^{F_1} \cong y_i^{F_2}, \theta_1^{F_1} \cong \theta_1^{F_2} \right\} \tag{16}$$

The final form of the distance between the fingerprint feature vectors is obtained by combining the formulas (15) and (16).

4. Feature vector classification and verification techniques

Fingerprint classification is performed using a template matching procedure [11,12]. We propose a supervised classifier for fingerprint feature vectors, that uses the minimum average distance [11].

Let us consider a set of input fingerprint images $\{F_1,...,F_n\}$ to be authenticated. We create a training set using the fingerprints of N authorized persons of the system. A set of fingerprints, named templates, are registered for each authorized user.

The training set will have the form $\left\{\left\{T_j^i\right\}_{j=1,...,n(i)}\right\}_{i=1,...,N}$, where T_j^i represents the jth template of the ith registered user, and $n(i)$ is the number of templates corresponding to that user. The feature vectors, $V(F_i)$, and the training vectors, $V(T_j^i)$, are computed using the described feature extraction approach.

Each fingerprint is associated to the registered user corresponding to the minimum average distance between the fingerprint's feature vector and the training vectors of that user. Therefore, the class of the current input fingerprint is $C_{ind(j)}$, where

$$ind(j) = \arg\min_{i\in[1,N]} \frac{\sum_{k=1}^{n(i)} d(V(F_j), V(T_k^i))}{n(i)}, \forall j \in [1, n] \tag{17}$$

and distance function d is given by (15). The N fingerprint classes, $C_1,...,C_N$, corresponding to the authorized persons, represent the identification result. Next, a fingerprint verification process has to be performed, to validate these identifications [8]. The verification procedure is modeled as :

$$\forall i \in [1, N], \forall F \in C_i : \frac{\sum_{j=1}^{n(i)} d(V(F), V(T_j^i))}{n(i)} > T \Leftrightarrow C_i = C_i \setminus \{F\} \tag{18}$$

where T represents a properly selected threshold value. Therefore, an identified fingerprint is excluded from a class of a registered user if the mean distance corresponding to that user is not low enough. The excluded fingerprints are labeled as *non-authorized person*.

5. Experiments

We have performed many fingerprint recognition experiments using the proposed authentication approach. We have obtained satisfactory results, achieving a high recognition rate, of approximately 90%, which prove the efectiveness of the described recognition technique.

We have used one of the FVC2004 fingerprint databases in our research. It contains 80 fingerprints of 10 different fingers, and was created using low cost fingerprint scanners [12].

Our approach produces a low number of false positives and false negatives (missed hits), obtaining high values for the performance parameters such as

Precision, *Recall* (almost 1) and the combined F_1 measure. Also, we have compared this minutiae-based technique with a pattern-based fingerprint recognition proposed by us [5], and found it provides a lower execution time and better recognition results.

5. Conclusions

A supervised minutiae-based fingerprint authentication system has been proposed in this paper. Our previous works in this domain approached the pattern-based fingerprint recognition [5]. This research focuses on the minutia point matching process [4,6-8].

We have used a binarization and thining based minutia detection procedure. Then, we have developed mathematical models for fingerprint feature extraction, fingerprint feature vector supervised classification and fingerprint verification.

Also, we have created a new special metric for computing the distance between fingerprint feature vectors and demonstrate its distance function properties. Our future work will focus on developing new metrics for fingerprint feature vector classification and new fingerprint matching solutions.

Aknowledgements

The research described here has been supported by the grant PNCDI II, IDEI program, CNCSIS Code 70/2008.

REFERENCES

[1] *L. C. Jain* et al., Intelligent Biometric Techniques in Fingerprint and Face Recognition, Boca Raton, FL: CRC Press, 1999.

[2] *S. Mazumdar, V. Dhulipala,* "Biometric Security Using Finger Print Recognition”, University of California, San Diego. 7 pages, Retrieved 30 August 2010.

[3] *J. Ravi, K. B. Raja, K. R. Venugopal,* “Fingerprint Recognition Using Minutia Score Matching”, International Journal of Engineering Science and Technology, Vol.1 (2), pp. 35-42, 2009.

[4] *H. Costin, I. Ciocoiu, T. Barbu, C. Rotariu*, “Through Biometric Card in Romania: Person Identification by Face, Fingerprint and Voice Recognition”, International Journal of Biomedical Sciences, Volume 1, Number 4, pp. 264-269, 2006.

[5] *A. Tudosă, M. Costin, T. Barbu, “*Fingerprint Recognition using Gabor filters and Wavelet Features”, Scientific Bulletin of the Politehnic University of Timisoara, Romania, Transactions on Electronics and Communications, Tom (49) 63, Fasc. 1, pp. 328-332, 2004.

[6] *V. Espinosa*, “Minutiae Detection Algorithm for Fingerprint Recognition”, Proc. of XXXV International Carnahan Conference on Security Technology, pp. 264-266, 16-19 October 2001.

[7] *D. Maio, D. Maltoni,* “Direct Gray-Scale Minutiae Detection in Fingerprints”, Journal IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 19 Issue 1, January 1997.

[8] *F. A. Afsar, M. Arif, M. Hussain*, “Fingerprint Identification and Verification System using Minutiae Matching”, Proc. of the National Conference on Emerging Technologies, 2004.

[9] *E. R. Dougherty*, An Introduction to Morphological Image Processing, ISBN 0-8194-0845-X 1992.

[10] *M. Sonka, V. Hlavac, R. Boyle*, Image Processing, Analysis, and Machine Vision, 2nd Edition, Pws. Pub. Co, 1998.

[11] *R. Duda, P. Hart, D. G. Stork*, Pattern Classification, John Wiley & Sons, 2000.

[12] *D. Maltoni, D. Maio, A. K. Jain*, *S. Prabhakar*, Handbook of Fingerprint Recognition (Second Edition), Springer, London, 2009.