Identification of an individual in a biometric system Fingerprint Technique

Mohammed Boutalline
Systems Engineering Laboratory
Sultan Moulay Sliman University
Beni Mellal, Morocco
boutalline@gmail.com

Hassan Faouzi
Sultan Moulay Sliman University
Beni Mellal, Morocco
faouzi.hassan.mi@gmail.com

Hamzaoui Radoine
Innovation Laboratory in Mathematics, Applications & Information Technologies
Sultan Moulay Sliman University
Beni Mellal, Morocco
info.hamzaoui@gmail.com

Belaid Bouikhalene
Innovation Laboratory in Mathematics, Applications & Information Technologies
Sultan Moulay Sliman University
Beni Mellal, Morocco
b.bouikhalene@usms.ma

Mohamed Fakir
Information Processing and Decision Support Laboratory
Sultan Moulay Sliman University
Beni Mellal, Morocco
m.fakir@usms.ma

***Abstract*—The fingerprints based about minutiae correspond essentially to the terminations and bifurcation of fingerprint patterns. Since the quality of fingerprint images is often low, automatic minutiae detection is a very difficult task and the extraction algorithms produce a large number of false alarms. A complete minutiae extraction scheme for automatic fingerprint recognition systems is presented. A great deal of work has been dedicated to fingerprint enhancement and to minutiae extraction. A new approach to combine different extraction algorithms is presented. The methods proposed, as confirmed by our simulations, allows an acceptable overall performance to be achieved.**

Keywords— Biometric system, fingerprints, minutiae, extraction, minutia matching.

I. INTRODUCTION

A. General

Biometrics is a set of mathematical analysis of biological characteristics of a person (biometric technologies) that use human characteristics such as physical or behavioral fingerprint, signature, iris, voice, face, approach, and a hand gesture at the end to determine his identity conclusively. It also proves as a powerful tool for identification / verification to scenes such as ATMs, doors, scene of the crime in the legal sector.

The fingerprint recognition is a mature biometric application for any identification or verification of individuals. In this document describes the design and development of an automatic identity authentication by fingerprint. This system of fingerprint recognition is based on a series of complex algorithms related to the fields of image processing and / or recognition of patterns.

The systems are increasingly found in applications related to security such as access control. There are always at least two modules in a biometric system: the learning module and the recognition (figure.1).

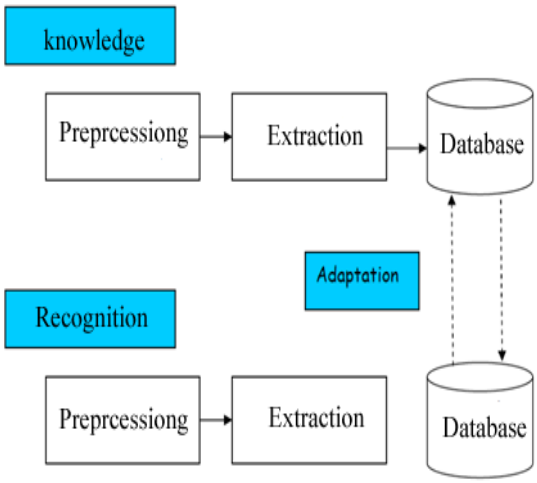


FIGURE 1. WORKING OF A BIOMETRIC SYSTEM

B. Fingerprint

Regarding the fingerprint, the British F. Galton [2] showed that in 1888 the first permanent design papillary birth to death, and unaltered. This particular arrangement of the papillary lines forms characteristic points, called minutiae, which are the cause of the individuality of digital designs.

A fingerprint consists of a lot of wrinkles and valleys. These wrinkles are characterized by minutiae. The figure.2 illustrates the types of minutiae.

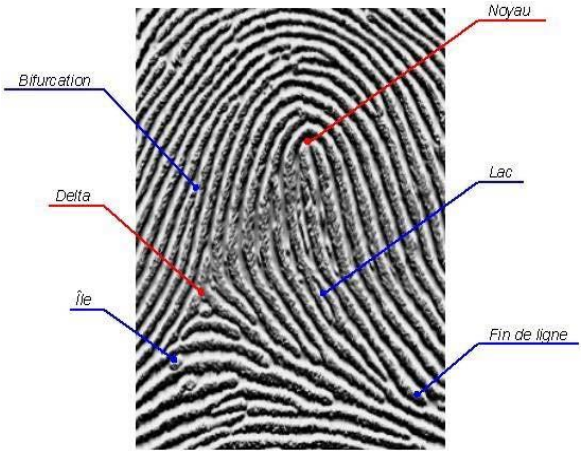


FIGURE.2. 6 MAIN TYPES OF MINUTIAE

The types of minutiaes reported in the literature, two types are the most used are stopping ride, the end of a ride, and the bifurcation, and the point on the ride in which two branches are derived (figure.3)

FIGURE.3. TWO TYPES OF MINUTIAES USED IN THE LITERATURE

C. *Overview of different approaches*

In general there are classes of algorithms for fingerprint recognition: The first category includes algorithms rather "conventional" that are based on the relative position of each minutiae, while the second contains algorithms to extract other features of the fingerprint such as the local management of ridges [3] and [4], or the frequency components of the local texture in the heart of the image [5]. The following diagram (figure.4) illustrates the steps of recognition of the fingerprint.

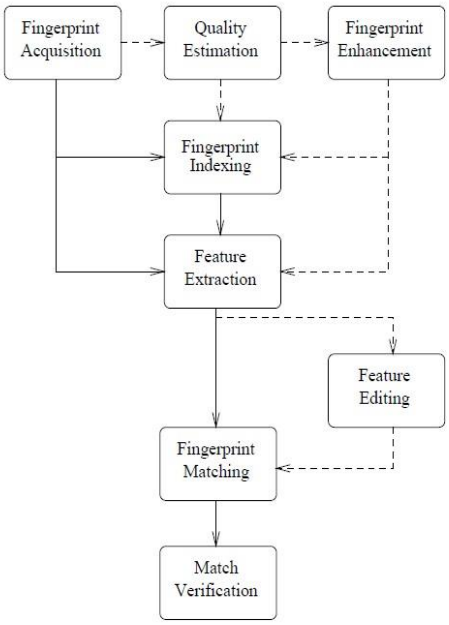


FIGURE.4. DESIGN OF A BIOMETRIC SYSTEM BASED ON FINGERPRINTS.

The approach, belonging to the first category is that proposed by A.K Jain [6] which is probably the best known. Is performed successively directional filtering and binarization of the image, the thinning (or skeletonization) of the ridges (figure.5), then determines the position of minutiae within the image to quantify the characteristics of similarity between two templates by « point pattern matching ».

FIGURE.5. PREPROCESSING OF FINGERPRINT IMAGES TO MINUTIAE EXTRACTION

II. RECOGNITION ALGORITHM

A. *Preprocessing*

The first step toward improving the image of the fingerprint using the Gabor filter [11], the binarization and skeletonization. The aim of this treatment is to obtain an image of the orientation of the grooves of the fingerprint. In other words, is assigned to each pixel of the image orientation of the ridge which it belongs. The calculation of the orientation takes place the following proposed by Jain Anil et Al [10]:

$$V_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{i+\frac{w}{2}} (2G\ (u,v) G_y(u, \quad (1)$$

$$V_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{i+\frac{w}{2}} (G^{\ 2}(u,v) - {G_y}^2 \quad (2)$$

$$\theta(i,j) = \frac{1}{2} tan^{-1}\left(\frac{V_x(i,j)}{V_y(i,j)}\right) \quad (3)$$

With

- W is the size of local window;
- Gx and Gy are the gradient magnitudes in directions of x and y, respectively
- θ(i,j) is the local orientation of the pixel (i,j)

The second step is to share the directional image into sub blocks (W*W pixels) and characterize them by an average orientation (among the eight directions defined) and only one, as determined by histogram calculation what is the direction that occurs most frequently within each block. Then filtered the original image at each point by applying a directional convolution [11] (2D Gabor filters) based on the average direction of lines (power steering) previously calculated. After filtering, the different ridges and valleys by binarization. This is a local binarization (threshold in a block of pixels W * W) to overcome the non-uniformity of intensity over the entire image. Finally pre-treatment of the fingerprint image, a skeletonization is achieved, comparable to a thinning operation. The effectiveness of such an algorithm for thinning is difficult to quantify, our choice was guided by the experiments summarized in Table 1: they compare two similar algorithms (based on morphological iterative methods) skeletonization and highlight the many benefits of the approach « Zhang » [8] compared to that of « Shapori » [9].

TABLE I. EXPERIMENTAL COMPARISON OF ALGORITHMS FOR SKELETONIZATION OF ZHANG AND SHAPORI

	Shapori	Zhang
		
		

B. Minutiaes extraction

The representation of attributes of the fingerprint is the most crucial phase in the design of a verification system. Representation clearly determines the accuracy. Existing systems are based on the minutiae of details.

The minutiae of the fingerprint are extracted from its skeleton by computing the "connectivity" CN at each point of the image P [1] as follows:

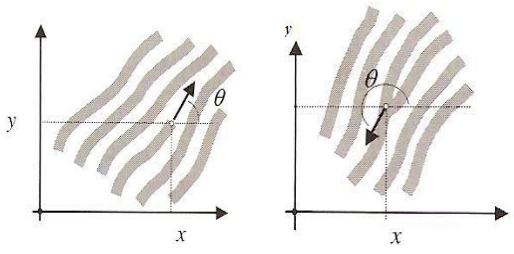
$$cn(p) = \frac{1}{2} \sum_{i=1\ldots8} val(P_{i \bmod 8}) - val(P_{i-1}) \quad (4)$$

P9 = P1, Pi is the value of pixels in the neighborhood 3*3 of P. Indeed the coefficient CN has characteristics (Table 2) that identify the nature of a detail according to the result obtained in the calculation of CN.

TABLE II. IDENTIFICATION OF A MINUTIAE FROM THE NC CALCULATION

CN	Nature of the minutiae in P
0	Error => Point isolé
1	Termination
2	Error => Through the ridge
3	Bifurcation
4	Error => Defining a more complex minutiae.

Bifurcations and endings are two types of minutiae used the most because they are easily detectable (Figure.6). The information in each detail of a fingerprint are then included in a vector form (type of minutiae, x, y,θ), which is a convenient way to save the information of a fingerprint on a computer.



a) Representation of a termination. *(b) Representation of a bifurcation.*

FIGURE.6. DETERMINING THE DIRECTION OF THE MINUTIAE

Upon execution of this stage all the minutiae will be found but the presence of false minutiae due to the acquisition that is not flawed then the next step is

necessary to eliminate these minutaes. These will be eliminated in the post-processing step following simple rules of structures can be used to detect many false minutiae that generally affect thinned binary fingerprint images. Xiao and Raafat (1991b) [7] identified the common false minutiae structures and introduces an approach to the neighbor to remove (Figure.7).

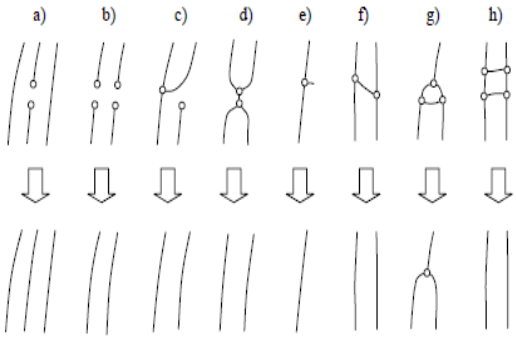


FIGURE.7. STRUCTURE OF THE MOST COMMON FALSE MINUTIAE

C. Comparison of minutiae

The comparison of a fingerprint with a database is to achieve agreement between a fingerprint image from a recording sheet (sheet 10 where the police are inked finger prints) and a latent, using minutiae.

The identity authentication system is based on comparing two sets of minutes, corresponding respectively to two fingers to compare. To determine whether two sets of minutiae extracted from two images correspond to the same finger prints, it is necessary to adopt a benchmarking system which is insensitive to possible translations, rotations and deformations that affect systematically fingerprints (Figure.8). From the same fingerprint, the calculation will never give 100% similarity due to the acquisition of two fingers (small deformations or displacements or rotations that affect systematically fingerprints).

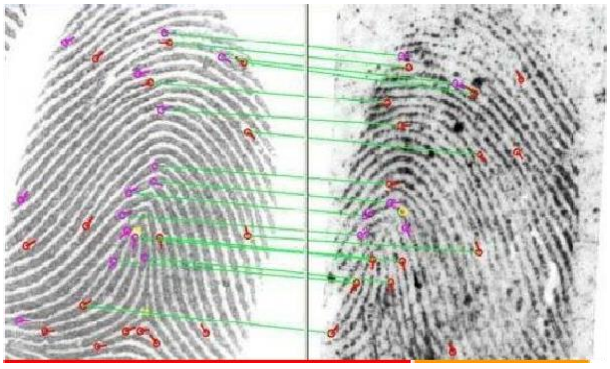


FIGURE.8. COMPARISON TEST WITH A MARKED TEMPLATE DATABASE

In the classification stage we used the method based on Euclidean distance, so to get it set up a test database containing the features extracted by the same method of learning and after it traverses the database of learning by calculating the Euclidean distance of the polar coordinates of the test image and the images of the database of learning, and the minimum distance will be that corresponding to the desired fingerprint.

$$d(x,y) = \sqrt{\sum_{i}^{N} (x_i - y_i)^2} \tag{5}$$

III. RESULTS AND CONCLUSION

Biometric work presented in this paper have led to the development of a system of identifying individuals by fingerprint recognition which the authentication phase itself (compare the clouds of minutiae).

To validate the system we worked on 50 tracks from five different people, 50% of prints were used for the learning phase, and 50% were used for tests to evaluate system performance.

Encouraging results appear. Indeed, the 50 tracks played, 44 were recognized, a recognition rate of 88%.

IV. BIBLIOGRAPHY

[1] Anil Jain et al.,2000, Automated Fingerprint Identification and imagingDavideMaltoni, Dario Maio, Anil K. SalilPrabhakar , 2003, Fingerprint Handbook

[2] Francis Galton, Fingerprint, McMillan, London, 1892.

[3] U. Halici et G. Onguin. *Fingerprint classification through self-organizing feature maps modified to treat uncertainties*. Proceedings of the IEEE, Vol. 84, n° 10,Octobre 1996.

[4] R. Capelli, A. Lumini, D. Maio et D. Maltoni. *Fingerprint classification by directional image partitioning*. IEEE Transactions on pattern analysis and machine intelligence, Vol. 21, n° 5, Mai 1999.

[5] A.K. Jain et S. Pankanti. *FingerCode: a filterbank for fingerprint representation and matching*. IEEE, 1999.

[6] A.K. Jain, L. Hong, S. Pankanti et R. Bolle. *An identityauthenfication system using fingerprints.* Proceedings of the IEEE, Vol. 85, n° 9, Septembre 1997.

[7] Xiao and Raafat (1991b). Xiao Q. and Raafat H., "Fingerprint image post-processing: A combined statistical and structural approach,"*Pattern Recognition*, vol. 24, no. 10, pp. 985–992, 1991b.

[8] J.R. Parker. *Algorithms for image processing andcomputer vision*. Wiley & Sons, Novembre 1996.

[9] Haralick, Robert et Shapiro. *Computer and robot vision*. Vol. 1, Addison-Wesley, 1992.

[10] Anil Jain et al.,2000, Automated Fingerprint Identification and imaging

[11] http://fr.wikipedia.org/