Retinal Angiography Based Authentication

C. Mariño[1], M.G. Penedo[1], M.J. Carreira[2], and F. González[3]

[1] Dep.Computación,Universidade da Coruña,
15781 A Coruña, castormp@fi.udc.es, cipenedo@dc.fi.udc.es
[2] Dep.Electrónica e Computación, Fac.Física de Santiago de Compostela,
15782 Santiago de Compostela, mjose@dec.usc.es
[3] Dep.Fisiología, Servicio de Oftalmología,
Centro Hospitalario Universitario de Santiago,
15782 Santiago de Compostela, fspaco@usc.es

Abstract. Traditional authentication (identity verification) systems, employed to gain access to a private area in a building or to data stored in a computer, are based on something the user *has* (an authentication card, a magnetic key) or something the user *knows* (a password, an identification code). But emerging technologies allow for more reliable and comfortable for the user, authentication methods, most of them based in biometric parameters. Much work could be found in literature about biometric based authentication, using parameters like iris, voice, fingerprint, face characteristics, and others. In this work a novel authentication method is presented, and first results obtained are shown. The biometric parameter employed for the authentication is the retinal vessel tree, acquired through a retinal angiography. It has already been asserted by expert clinicians that the configuration of the retinal vessels is unique for each individual and that it does not vary in his life, so it is a very well suited identification characteristic. Before the verification process can be executed, a registration step is needed to align both the reference image and the picture to be verified. A fast and reliable registration method is used to perform that step, so that the whole authentication process takes very little time.

1 Introduction

Reliable authentication of people has long been an interesting goal, becoming more important as the need of security grows, so that access to a reliable personal identification infrastructure is an essential tool in many situations (airport security controls, all kinds of password-based access controls, ...). Conventional methods of identification based on possession of ID cards or exclusive knowledge are not altogether reliable. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised. A solution to that problems has been found in the biometric based authentication technologies. A biometric system is a pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user. Identification can be in the form of verification, authenticating a claimed identity, or recognition, determining the

A. Sanfeliu and J. Ruiz-Shulcloper (Eds.): CIARP 2003, LNCS 2905, pp. 306–313, 2003.

identity of a person from a database of known persons (determining who a person is without knowledge of his/her name).

Many authentication technologies can be found in the literature, with some of them already implemented in commercial authentication packages [1]. Other methods are the fingerprint authentication [2][3] (perhaps the oldest of all the biometric techniques), hand geometry [4], face recognition [5] or speech recognition [6]. It also has been shown that for a more reliable system, combination of two or more of those techniques could be good choice [7].

But today the most of the efforts in authentication systems tend to develop more secure environments, where it is harder, or ideally, impossible, to create a copy of the properties used by the system do discriminate between authorized individuals and unauthorized ones,so that an impostor could be accepted by the biometric system as a true sample.

In that sense, the system proposed here employs for authentication biometric parameter the blood vessel pattern in the retina of the eye: it is a unique pattern in each individual, it is almost impossible to forge that pattern in a false individual. Of course, the pattern is the same since the person is born until she dies, at least it appears a pathology in the eye. In `http://www.eye-dentify.com` a commercial authentication system is available, where characteristic points extracted from the vessels are used to measure the similarity between images. Here a novel authentication method based in the whole retinal vessel pattern of the eye is presented, and first results obtained with that technique are shown. In the first section, a brief outline about image registration is presented, because of the necessity of a prior alignment of the images to be compared. Second section describes the system developed in our laboratory to test the accuracy of our method, and in the third section an experiment run in collaboration with the University Hospital of Santiago and results obtained are shown. Finally conclusions and future lines are included as a closing section.

2 Methodology

2.1 Image Registration

In many cases it is almost impossible to acquire the biometric parameter in the same conditions than the stored template used for the authentication, so that a first step of normalization of both parameters (the acquired and the reference one) is needed in order to make the system reliable enough, avoiding the rejection of legitimate users by changes due to illumination, translations or rotations in the image. The main drawback of retinal angiographies is the different position of the vessels used in the authentication, because it is very difficult that the user place the eye in the same position in different acquisitions, so that an alignment is necessary prior to the authentication. To perform that alignment, an image registration algorithm is employed.

Image registration consists in estimating the transformation $\hat{T}$ (we will only consider affine transformations) that aligns two images so that the points in one image can be related to points in the other. To determine the optimal transformation an iterative process is performed so that a similarity measure is optimized.

There is a lot of image registration methods (see [8][9] for complete surveys about them). The registration method developed for the alignment of the images employed in the authentication process have been widely described in [10][11], but for the sake of convenience a brief outline will be included in the following subsection.

Creaseness based registration method. Vessels can be thought as creases (ridges or valleys) when images are seen as landscapes. Amongst the many definitions of crease, the one based on level set extrinsic curvature (LSEC) has useful invariance properties. Given a function $L : \mathcal{R}^d \rightarrow \mathcal{R}$, the level set for a constant l consists of the set of points $\{\mathbf{x}|L(\mathbf{x}) = l\}$. For $2D$ images, L can be considered as a topographic relief or landscape and the level sets are its level curves. Negative minima of the level curve curvature κ, level by level, form valley curves, and positive maxima ridge curves.

$$\kappa = (2L_xL_yL_{xy} - L_y^2L_{xx} - L_x^2L_{yy})(L_x^2 + L_y^2)^{-\frac{3}{2}} \tag{1}$$

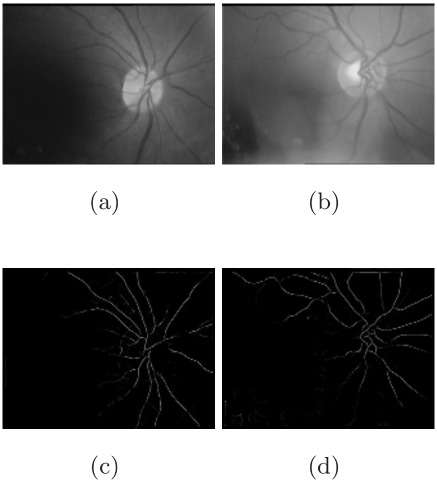
However, the usual discretization of LSEC is ill–defined in a number of cases, giving rise to unexpected discontinuities at the center of elongated objects. Instead, we have employed the $MLSEC - ST$ operator, as defined in [12]. This alternative definition is based on the divergence of the normalized vector field $\bar{\mathbf{w}}$:

$$\kappa = -\text{div}(\bar{\mathbf{w}}) \tag{2}$$

Although equations (1) and (2) are equivalent in the continuous domain, in the discrete domain, when the derivatives are approximated by finite centered differences of the Gaussian–smoothed image, equation (2) provides much better results.

After the extraction of the vessel landmarks (see figure 1 (c) and (d)), the straightest approach is to perform an iterative optimization of some alignment function: one image is taken as reference, while the other is iteratively transformed until the function attains a hopefully global maximum. As the optimization function, Downhill Simplex Iterative algorithm was selected, as implemented in [13], and for alignment, the linear correlation function.

But this straight approach works only for almost-aligned and identical content images; the common case is that the optimization gets trapped in a local maximum. Therefore, some sort of exhaustive search for most promising seeds must be performed before the Simplex search starts. An efficient way to do it is in the Fourier domain, employing a well known property which relates a multiplication in this domain to the values of linear correlation. Furthermore, in order to overcome the time bottleneck that this computation demands, we build a pyramid for each image, where each level is a sampled version of a local maximum of the previous level. The exhaustive search is computed only at the top (smaller) image, which greatly reduces the computation time. The method is more widely described in [14][10].



(a) (b)

(c) (d)

Fig. 1. Two examples of retinal angiographies, where variation between individuals can be seen. Images in (c) and (d) depict the extracted vessels of (a) and (b) respectively.

2.2 Retinal Based Authentication

Once the registration process has been performed and images are aligned, extracted registered creases images are utilized to obtain a similarity measure between them. So, if two images belong to the same person, aligned creases images will be more similar than images from different persons, although the registration process is successfully performed. The measure employed must be robust against changes in image amplitude such as those caused by changing lighting conditions, and also against the number of points obtained in the creases extraction process. Such conditions are fulfilled by the Normalized Cross-Correlation coefficient (NCC), that is defined as [15]:

$$\gamma = \frac{\sum_{x,y}[f(x,y)-\overline{f}][t(x,y)-\overline{t}]}{\left\{\sum_{x,y}[f(x,y)-\overline{f}]^2\sum_{x,y}[t(x,y)-\overline{t}]^2\right\}^{0.5}} \tag{3}$$

where $\overline{t}$ is the mean of the registered image, and $\overline{f}$ is the mean of the image. It must be noted that although the sums are over all of the images, only the overlapping areas of them are not null (as depicted in Figure 2, where the original and the registered images are shown).

Once calculated the normalized correlation coefficient γ, a confidence measure must be determined to know if two images belong to the same person. To avoid false acceptance cases caused by errors in the acquisition, where only small creases could be extracted, an acquired image is considered valid for the authentication algorithm if the number of points in the creases is above a minimum

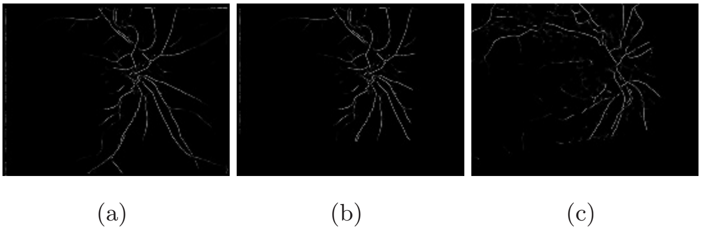


Fig. 2. (a) Original with no overlapping area creases image, (b) cropped original with only the overlapping area creases image and (c) registered creases image. Only overlapping area of the images are not null

number of points. That threshold is obtained by the application of the Tchebycheff theorem [16]: if the number of points in the creases N_c fulfills that $N_c > 3\sigma$, where σ is the mean number of points in the creases of a set of well acquired images, then the image will be considered as valid image for the system, but if $N_c < 3\sigma$ then the image will be rejected by the system.

3 Method Validation and Results

Images employed in our experiments were acquired in a period of 15 months and in different centers of the University Hospital of Santiago de Compostela (CHUS), although all of them with the same camera, a Cannon CR6-45NM Non-Mydriatic Retinal Camera, with a resolution of 768×584 pixels. Although originally they were color images, a conversion to gray-level images was performed prior to the storage in the database, since color does not provide any useful information.

First experimental results showed that the value of the *NCC* of the images belonging to the same individual, although acquired in different times, is always above the value 0.6. In that first experiments, a set of 4 images from 5 different persons (20 images) were evaluated by the system.

To test the reliability of our system, a bigger blind experiment was designed in collaboration with the CHUS: a set of 119 retinal angiographies was introduced in the system. In the benchmark two kind of images could be found: the more of the images (110) belonged to different individuals, and a reduced number of them (6 from 3 individuals, 2 of each) were images from the same persons taken in different times. The system should be able to find the images in the benchmark which pertain to the same persons.

In the test, the *NCC* of the cartesian product of the set of 116 images was calculated (three images were eliminated from the total of 119 because they presented very poor contrast, so creases were too small and were refused by the system as described above). The value of the *NCC* of the rest of images was normalized to the interval $[0, 1]$, as can be seen in the figure 3. It is clear that the values of the diagonal of that image are all 1, since it belongs to the correlation of the images with themselves. The other values belong to the other two categories: values bigger than 0.6 are obtained correlating images pertaining to the same person but acquired in different moments, and the rest of the values, which are all of them under the peak value 0.35 corresponds to the value of the *NCC* of images of different individuals. That way, to verify the identity of an individual, the system only has to search in the set of stored templates, and if the value of the *NCC* is below a confidence level for all the correlation values, the person will not gain permission to get into the protected area or to read the information.

The confidence level represents a very important parameter in the system, since a too low level would lead the system to accept even false individuals, but a too high level would reject legitim individuals. Figure 4 shows the percentages of false rejection and false acceptance cases. It can be clearly seen in that figure that until the threshold value is 0.60, true positive cases percentage is 1, meaning that no true positive is rejected. From that point until the threshold is 1 the acceptance cases are just the values from the *NCC* of each image with itself, which is always 1.0. In the opposite side, when the threshold goes down, false negative cases does not appear until its value is 0.35, growing exponentially from that point. From this values, when the threshold value is in the range from 0.35 to 0.60 the successful percentage of the system is 100%.

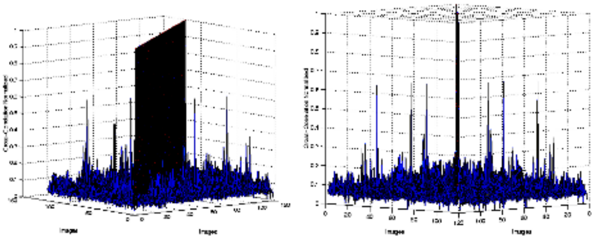


Fig. 3. Two views of a graph representing the values of the correlation obtained in the experiment with 119 images. Main diagonal is always 1, since it corresponds to *NCC* of each image with itself, and the other peaks with value 0.6 correspond to the correlation of images from the same person taken in different moments.

All the conclusions exposed in this work were tested by the expert clinicians of the CHUS, since they knew before the experiment was performed, which images belonged to the same individuals, and which were not, concluding that results were right, and that matching images were effectively taken from the same patients, and that did not exist false rejections, so the system got, for this first tests, a 100% of success.

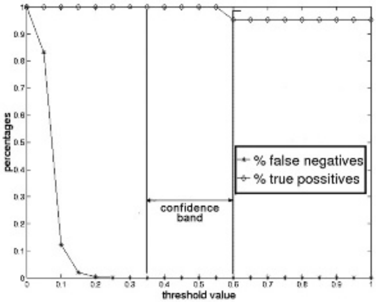


Fig. 4. Percentages of false acceptance and false rejections when the threshold level is varied.

4 Conclusions and Future Lines

A novel authentication method has been presented here. The authentication procedure employs the retinal vessel tree as the biometric parameter, with a prior registration stage needed to align the template image and the acquired image. To measure the similarity between the images, Normalized Cross Correlation of the aligned creases extracted from the images is used. The technique has been extensively tested, with a test that involved 14.161 cases, giving very good results. It must be noted that the registration method employed here is coherent [17], since the result obtained from the registration of image I_1 registered against I_2 is the same than the result obtained using I_2 as the reference image (figure 3). From that experiment, it can be assessed that *NCC* could be used as a robust measure of the similarity of the images, with values over 0.6 for the 127 cases of images from the same person, and values under 0.35 for the 14034 images which belong to different individuals. Moreover, an analysis of the behavior of the system when the acceptance threshold is varied is presented, so that it can be seen that a wide band of 0.35 in the *NCC* appears between the acceptance area and the rejection area. The mean time taken to perform each image authentication is 0.3 seconds, 0.26 seconds for the registration and 0.04 seconds to perform the computation of the *NCC* value, so that the method is very well-fitted to be employed in a real authentication system.

Future research will include the development of a hardware system based on the technique presented here which will improve performance until almost real time authentication.

Acknowledgements. This paper has been partly funded by the Xunta de Galicia through the grant contract PGIDT01PXI10502PR.

References

1. J.G. Daugman. Biometric personal identification system based on iris analysis. United States Patent No.5,291.560, 1994.
2. Federal Bureau of Investigation. The science of fingerprints: Classifications and uses. Technical report, U.S.Government Printing Office, Washington D.C., 1984.
3. A. Jain, L. Hong, S. Pankanti, and R. Bolle. An identity authentication system using fingerprints. *Proceedings of the IEEE*, 85(9), September 1997.
4. R. Zunkel. Hand geometry based verification. In *BIOMETRICS:Personal Identification in Networked Society*. Kluwert Academic Publishers, 1999.
5. W. Zhao, R. Chellappa, A. Rosenfeld, and P. Phillips. Face recognition: A literature survey. Technical report, National Institute of Standards and Technology, 2000.
6. J.Bigüin, C.Chollet, and G.Borgefors, editors. *Proceedings of the 1st.International Conference on Audio- and Video-Based Biometric Person Authentication*, Crans-Montana,Switzerland, March 1997.
7. Patrick Verlinde, Gerard Chollet, and Marc Acheroy. Multi-modal identity verification using expert fusion. *Information Fusion*, 1(1):17–33, 2000.
8. L.G. Brown. A survey of image registration techniques. *ACM Computer Surveys*, 24(4):325–376, 1992.
9. J.B.A. Maintz and M.A. Viergever. A survey of medical image registration. *Medical Image Analysis*, 2(1):1–36, 1998.
10. D. Lloret, C. Mariño, J. Serrat, A.M. López, and J.J. Villanueva. Landmark-based registration of full slo video sequences. In *Proceedings of the IX Spanish Symposium on Pattern Recognition and Image Analysis*, volume I, pages 189–194, 2001.
11. C. Mariño, M. Penas, M.G. Penedo, D. Lloret, and M.J Carreira. Integration of mutual information and creaseness based methods for the automatic registration of slo sequences. In *Proceedings of the SIARP'2001, VI Simpósio Ibero-Americano de Reconhecimento de Padrões*, volume I, 2001.
12. A. López, D. Lloret, J. Serrat, and J.J. Villanueva. Multilocal creasness based on the level set extrinsic curvature. *Computer Vision and Image Understanding*, 77:111–144, 2000.
13. W. Press, S. Teukolsky, W. Vetterling, and B. Flannery. *Numerical Recipes in C.* Cambridge University Press, 2 edition, 1992.
14. D. Lloret, A. López, J. Serrat, and J.J. Villanueva. Creaseness-based CT and MR registration: comparison with the mutual information method. *Journal of Electronic Imaging*, 8(3):255–262, July 1999.
15. J.P.Lewis. Fast template matching. *Vision Interface*, pages 120–123, 1995.
16. S. Ehrenfeld and S.B. Littauer. *Introduction to Statistical Method*, page 132. McGraw-Hill, 1964.
17. G.E.Christensen and H.J.Johnson. Consistent image registration. *IEEE Trans. on Medical Imaging*, 20(7):568–582, July 2001.