A NOVEL SIMILARITY METRIC FOR RETINAL IMAGES BASED AUTHENTICATION

M. Ortega, M. G. Penedo, C. Mariño
Department of Computer Science, University of A Coruña, A Coruña, Spain

M. J. Carreira
Department of Computer Science and Electronics, University of Santiago de Compostela, Santiago de Compostela, Spain

Keywords: Authentication System, Similarity Measure, Retinal Images, Biometric Pattern, Feature point matching.

Abstract: In biometrics the identity of an individual is verified using some physiologic or behavioural feature. In a typical authentication process involving some biometric trait, the biometric pattern for the user is extracted (a set of feature landmarks, a characteristic vector etc...). A similarity score is calculated between these patterns to determine if they belong to the same individual or not. This work presents an analysis of similarity metrics for an authentication system in which retinal vessel feature points are used as biometric pattern. The VARIA database of retinal images is used. A new metric is defined weighting the matched points information with the previously defined metrics. The obtained results show a large stretchment of the confidence gap between the matching scores of patterns from the same individual and the matching scores of patterns from different ones.

1 INTRODUCTION

Traditional authentication systems based on knowledge (a password, a pin) or possession (a card, a key) are not reliable enough for many environments, due to their common inability to differentiate between a true authorized user and an user who fraudulently acquired the privilege of the authorized user. A solution to these 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 behavioural characteristic.

Authentication technologies can be found in the literature using fingerprints (Jain et al., 1997; Tico and Kuosmanen, 2003) (perhaps the oldest of all the biometric techniques), face recognition (Zhao et al., 2000), speech (J.Bigüin et al., 1997)...

These biometrics systems typically rely the comparison between individuals on a matching of their own extracted patterns. This matching process has a major impact in the final effectiveness of the system. One of the typical pattern matchings is the point pattern matching, where some feature points or landmarks are extracted for the individuals using a biometric trait (fingerprints, retinal vessel tree...) and then both sets of points are compared. Once both sets are matched, it is important to establish a good similarity (or dissimilarity in some cases) metric value. This value is the ultimate criterion to distinguish between a client (authorized access) or an attack (unauthorized).

Retinal vessel tree pattern has been proved a valid biometric trait for personal authentication as it is unique, time invariant and very hard to forge, as showed in (Mariño et al., 2006) where a novel authentication system based on this trait was introduced. The whole arterious-venous tree structure was used as the feature pattern for individuals. One drawback of the proposed system was the necessity of storing and handling the whole vessel tree image as a pattern. Based on the idea of fingerprint minutiae (Jain et al., 1997), a more ideal and robust pattern was first introduced in (Ortega et al., 2006) where a set of landmarks (bifurcations and crossovers between retinal vessels) were extracted and used as feature points. In this scenario, the matching problem is a point pattern matching problem and the similarity metric is defined in terms of matched points.

In this work, similarity metrics are designed and analyzed for the retinal feature point based biometric system. These metrics emphasise the importance of

Ortega M., Penedo M., Mariño C. and Carreira M. (2009).
A NOVEL SIMILARITY METRIC FOR RETINAL IMAGES BASED AUTHENTICATION.
In *Proceedings of the International Conference on Bio-inspired Systems and Signal Processing*, pages 249-253
DOI: 10.5220/0001510602490253

the right classification in attacks and client accesses. The paper is organized as follows: in section 2 a brief description of the authentication system is presented, specially the feature points extraction and the matching stages. Section 3 deals with the analysis of several similarity metrics applied to this system. Section 4 shows the effectiveness results obtained by the metrics running a test images set. Finally, section 5 provides some discussion and conclusions.

2 AUTHENTICATION SYSTEM PROCESS

As previously commented, retinal vessel tree is a good biometric trait for authentication. To obtain a good representation of the tree, the creases of the image are extracted. As vessels can be thought of as ridges seeing the retinal image as a landscape, creases image will consist in the vessels skeleton (Figure 1(a) and 1(b)).

Using the whole creases image as biometric pattern has a major problem in the codification and storage of the pattern, as we need to store the whole image. To solve this, similarly to the fingerprint minutiae (ridges, endings, bifurcations in the fingerprints), a set of landmarks is extracted as the biometric pattern from the creases image. The most identifiable and invariant landmarks in retinal vessel tree are crossovers and bifurcation points and, therefore, they are used as biometric pattern in this work.

To detect feature points, creases are tracked to label all of them as segments in the vessel tree, marking their endpoints. Next, bifurcations and endpoints are extracted by means of relationships between segments. These relationships are found detecting segments close to each other and calculating their directions. If a segment endpoint is close to another segment and forming an angle smaller than $\frac{\pi}{2}$, a bifurcation or crossover is detected. Figure 1(c) shows the result obtained after this stage.

Once the biometric pattern for an individual, β, is obtained as a set of points, it has to be compared with the stored reference pattern, α, to validate the identity of the individual. Due to the eye movement during the image acquisition stage, it is necessary to align β with α in order to be matched. They may also have different cardinality. Considering the reduced range of eye movements during the acquisition, a Similarity Transform schema (ST) is used to model pattern transformations (N. Ryan and de Chazal, 2004). A search in the transformation space is performed to find the more suitable parameters of the alignment. Once both patterns are aligned, a point p from α and a point p' from

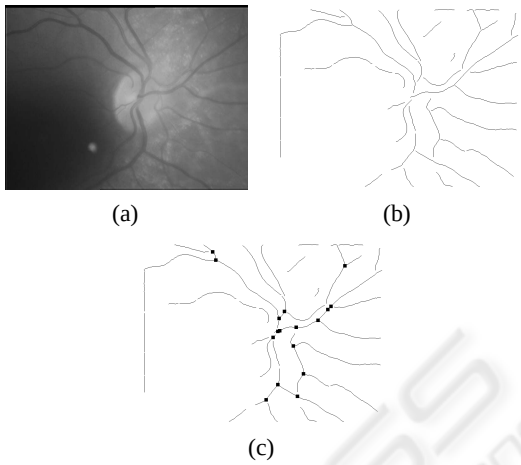

Figure 1: (a) original image (b) creases image (c) creases image with the feature points extracted from it.

β match if $distance(p, p') < D_{max}$, where D_{max} is a threshold introduced in order to consider the discontinuities during the creases extraction process leading to mislocation of feature points. This way, the number of matched points between patterns is calculated. Next, similarity metrics are established to obtain a final criterion of comparison between patterns.

3 SIMILARITY METRICS ANALYSIS

The main goal is to define similarity measures on the aligned patterns to correctly classify authentications in both classes: attacks (unauthorized accesses), when the two matched patterns are from different individuals and clients (authorized accesses) when both patterns belong to the same person.

For the metric analysis a set of 150 images (100 images, 2 images per individual and 50 different images more) from VARIA database (VARIA,) were selected. These images have a high variability in contrast and illumination allowing the system to be tested in quite hard conditions. In order to build the training set of matchings, all images are matched versus all the images (a total of 150x150 matchings). The matchings are classified into attacks or clients accesses depending if the images belong to the same individual or not. Separation of both classes by some metric determines its classification capabilities.

The main information to measure similarity between two patterns is the number of feature points successfully matched between them. Figure 2, shows histogram of matched points for both classes of authentications in the training set. As it can be observed,

matched points information is by itself quite significative but insufficient to completely separate both populations as in the interval $[10,13]$ there is an overlapping between them.

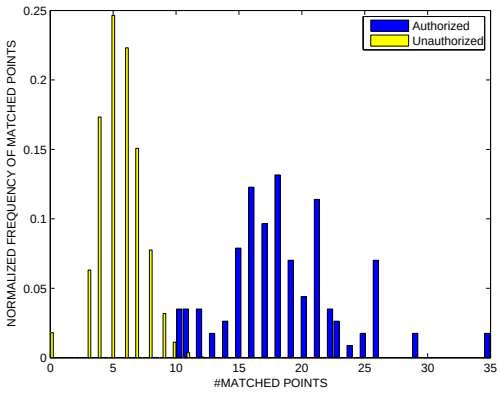

Figure 2: Matched points histogram in the attacks (unauthorized) and clients (authorized) authentications cases. In the interval [10,13] both distributions overlap.

To combine information of patterns size and normalize the metric, a normalization function will be used. The similarity measure (S) between two patterns will be defined by

$$S = \frac{C}{\sqrt{MN}} \tag{1}$$

where C is the number of matched points between patterns, and M and N are the matching patterns sizes.

Figure 3 shows distributions chart for our training set using the proposed metric in Equation 1. This metric combines both pattern sizes information allowing the system to reduce the similarity value in attacks involving small sized patterns while keeping

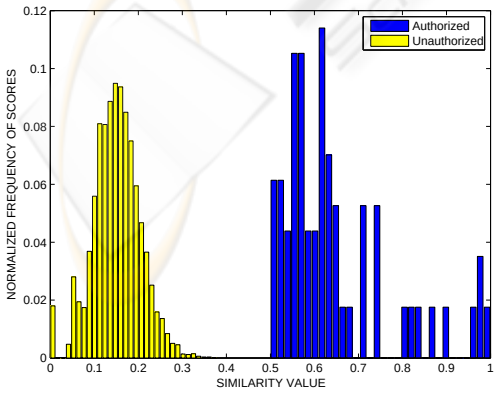

Figure 3: Similarity values distribution for authorized and unauthorized accesses using metric defined in Equation 1.

clients cases histogram in a similar range. A confidence band between both classes can be established now in $[0.38,0.5]$.

However, normalizing the metric has the side effect of reducing the similarity between patterns of the same individual where one of them has a much greater number of points than the other. To correct this situation, the influence of the number of matched points and the patterns size have to be balanced. A correction parameter (γ) is introduced in the similarity measure to control this situation. The new metric is defined as:

$$S_\gamma = S * C^{\gamma-1} = \frac{C^\gamma}{\sqrt{MN}} \tag{2}$$

where S, C, M and N are the same parameters from Equation 1. The γ correction parameter allows to improve the similarity values when a reasonable number of matched points is obtained specially in cases of patterns with many points.

In order to normalize the metric again to the $[0,1]$ interval, S_γ is divided by a reference value, R, representing a similarity value in the S_γ space which is certain to be an authorized access case. The new normalized metric will be defined as:

$$S_{\gamma R} = min\left\{\frac{S_\gamma}{R}, 1\right\} \tag{3}$$

R can be defined in the same space as S_γ in Equation 2 as $R = S_R * C_R^{\gamma-1}$, where S_R and C_R are values in the similarity and matched points space, respectively. Those values must have a very high probability to belong to a match between patterns from the same individual. Moreover, these parameters should not be very high in order to allow a good number of positive cases to get closer to a similarity value of 1.Ideally, mean values for the similarity and matched points distributions should be used.

In Figure 2 and 3, the distribution of the unauthorized and authorized cases can be observed for the matched points and normalized metric,respectively. Mean values for the clients accesses are, respectively, 18 and 0.65. Distributions for the unauthorized accesses have a mean and standard deviation values of $\mu_m = 5.58, \sigma_m = 1.74$ for matched points and $\mu_s = 0.1508, \sigma_s = 0.0537$ for similarity values.

Given that $18 > \mu_m + 7 * \sigma_m$ and $0.65 > \mu_s + 9 * \sigma_s$, $S_R = 0.65$ and $C_R = 18$ are values safe enough to be used as they are far enough from their respective attacks distributions means.

Finally, to choose a good γ parameter, the confidence band improvement has been evaluated for different values of γ (Figure 4). The maximum improvement is achieved at $\gamma = 1.12$ with a confidence band

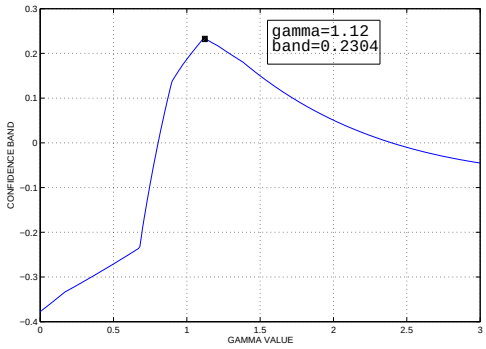

Figure 4: Confidence band size vs gamma (γ) parameter value. Maximum interval is obtained at $\gamma = 1.12$.

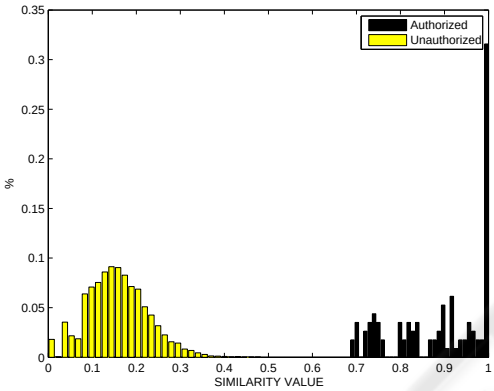

Figure 5: Similarity values distributions using the normalized metric with γ=1.12

of 0.2304, twice the original from previous section. Figure 5 shows the distributions values obtained for this metric with $\gamma = 1.12$.

4 RESULTS

A test set of 100 images (2 per individual), different from the training set has been built in order to test the metrics performance once their parameters have been fixed with the training set. Metrics performance is used by means of the FAR vs FRR graph like in the case of the ROC curves.

This graph displays two curves representing the evolution of the False Acceptance Rate (FAR) and False Rejection Rate (FRR) versus the value of the similarity decision threshold. In this case, a false acceptance is the acceptance of an attack and a false rejection is the rejection of a client. A typical performance parameter is the Equal Error Rate (EER) which indicates the rate where FAR = FRR. Figure 6 shows

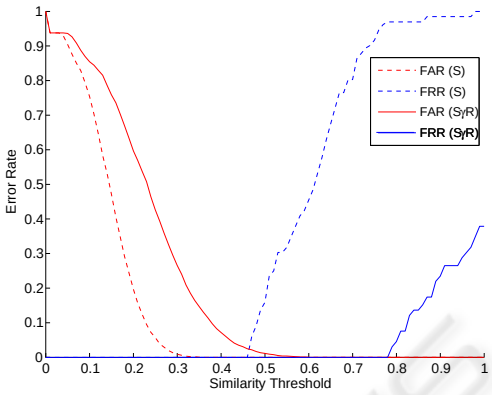

Figure 6: FAR vs FRR curves for the normalized similarity metrics S (Equation 1) and $S_{\gamma R}$ (Equation 3).

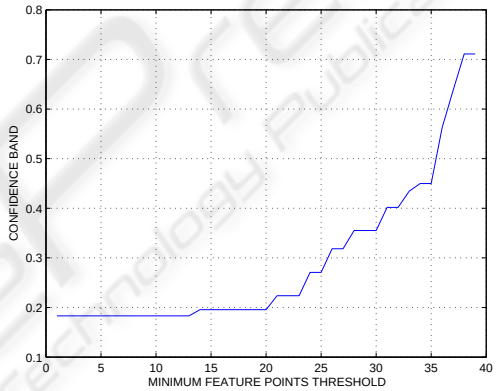

Figure 7: Confidence band evolution depending on the minimum points constraint.

FAR and FRR curves for metrics defined in previous section (the normalized metric defined in Equation 1 and the gamma-corrected normalized metric defined in Equation 3). The EER is 0 for the normalized and gamma corrected metrics as it was the same case in the training set, and, again, the gamma corrected metric shows the highest confidence band in the test set (0.195 vs 0.109).

Finally, to evaluate the influence of the image quality influence, in terms of feature points detected per image, a test is run where, images with a biometric pattern size below a threshold are removed for the set and the confidence band obtained with the rest of the images is evaluated. Figure 7 shows the evolution of the confidence band versus the minimum detected points constraint. The confidence band does not grow significatively until a fairly high threshold is set. Taking as threshold the mean value of detected points for all the test set (25.7), the confidence band grows from 0.1950 to 0.2701. Even removing half of the images,

the band only is increased by 0.075, suggesting that the gamma-corrected metric is highly robust to big quality image variations.

5 CONCLUSIONS AND FUTURE WORK

The performance of an authentication system based on feature points of the retinal vessel tree has been evaluated. Several metrics have been analyzed in order to test the classification capabilities of the system and a new weighted metric has been defined. The results are very good and prove that the defined authentication process is suitable and reliable for the task. The use of feature points to characterise the individuals is a robust biometric pattern and allow to define similarity metrics that offer a good confidence band. Moreover, to reduce the influence of low quality images a parameter γ is introduced to correct the influence of the absolute quantity of matched points.

Future work includes the use of high-level information of points to complete the metrics and a full quality image study to determine some constraints over the contrast and illumination values.

ACKNOWLEDGEMENTS

This paper has been partly funded by the Xunta de Galicia through the grant contracts PGIDIT06TIC10502PR.

REFERENCES

Jain, A., Hong, L., Pankanti, S., and Bolle, R. (1997). An identity authentication system using fingerprints. *Proceedings of the IEEE*, 85(9).

J.Bigüin, C.Chollet, and G.Borgefors, editors (1997). *Proceedings of the 1st.International Conference on Audio- and Video-Based Biometric Person Authentication*, Crans-Montana,Switzerland.

Mariño, C., Penedo, M. G., Penas, M., Carreira, M. J., and González, F. (2006). Personal authentication using digital retinal images. *Pattern Analysis and Applications*, 9:21–33.

N. Ryan, C. H. and de Chazal, P. (2004). Registration of digital retinal images using landmark correspondence by expectation maximization. *Image and Vision Computing*, 22:883–898.

Ortega, M., Mariño, C., Penedo, M. G., Blanco, M., and González, F. (2006). Personal authentication based on feature extraction and optical nerve location in digital retinal images. *WSEAS Transactions on Computers*, 5(6):1169–1176.

Tico, M. and Kuosmanen, P. (2003). Fingerprint matching using an orientation-based minutia descriptor. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(8):1009–1014.

VARIA. Varpa retinal images for authentication. http://www.varpa.es/varia.html.

Zhao, W., Chellappa, R., Rosenfeld, A., and Phillips, P. (2000). Face recognition: A literature survey. Technical report, National Institute of Standards and Technology.