Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2009, Article ID 235746, 13 pages
doi:10.1155/2009/235746

Research Article

Retinal Verification Using a Feature Points-Based Biometric Pattern

M. Ortega,[1] M. G. Penedo,[1] J. Rouco,[1] N. Barreira,[1] and M. J. Carreira[2]

[1] *VARPA Group, Faculty of Informatics, Department of Computer Science, University of Coruña, 15071 A Coruña, Spain*
[2] *Department of Electronics and Computer Science, University of Santiago de Compostela, 15782 Santiago de Compostela, Spain*

Correspondence should be addressed to M. Ortega, mortega@udc.es

Received 14 October 2008; Accepted 12 February 2009

Recommended by Natalia A. Schmid

Biometrics refer to identity verification of individuals based on some physiologic or behavioural characteristics. The typical authentication process of a person consists in extracting a biometric pattern of him/her and matching it with the stored pattern for the authorised user obtaining a similarity value between patterns. In this work an efficient method for persons authentication is showed. The biometric pattern of the system is a set of feature points representing landmarks in the retinal vessel tree. The pattern extraction and matching is described. Also, a deep analysis of similarity metrics performance is presented for the biometric system. A database with samples of retina images from users on different moments of time is used, thus simulating a hard and real environment of verification. Even in this scenario, the system allows to establish a wide confidence band for the metric threshold where no errors are obtained for training and test sets.

1. Introduction

Reliable authentication of persons is a growing demanding service in many fields, not only in police or military environments but also in civilian applications, such as access control or financial transactions. Traditional authentication systems are based on knowledge (a password, a pin) or possession (a card, a key). But these systems are not reliable enough for many environments, due to their common inability to differentiate between a true-authorised user and a user who fraudulently acquired the privilege of the authorised 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 is usually used in the form of verification (checking the validity of a claimed identity) or identification (determination of an identity from a database of known people, this is, determining who a person is without knowledge of his/her name).

Many authentication technologies can be found in the literature, some of them already implemented in commercial authentication packages [1–3]. Other methods are the fingerprint authentication [4, 5] (perhaps the oldest of all the biometric techniques), hand geometry [6], face [7, 8], or speech recognition [9]. Nowadays, 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 to discriminate between authorised and unauthorised individuals. [10–12].

This paper proposes a biometric system for authentication that uses the retina blood vessel pattern. This is a unique pattern in each individual and it is almost impossible to forge that pattern in a false individual. Of course, the pattern does not change through the individual's life, unless a serious pathology appears in the eye. Most common diseases like diabetes do not change the pattern in a way that its topology is affected. Some lesions (points or small regions) can appear but they are easily avoided in the vessels extraction method that will be discussed later. Thus, 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 by Mariño et al. [13, 14], who introduced a novel authentication system based on this trait. In that work, the whole arterial-venous tree structure was used as

the feature pattern for individuals. The results showed a high confidence band in the authentication process but the database included only 6 individuals with 2 images for each of them. One of the weak points of the proposed system was the necessity of storing and handling a whole image as the biometric pattern. This greatly facilitates the storing of the pattern in databases and even in different devices with memory restrictions like cards or mobile devices. In [15] a pattern is defined using the optic disc as reference structure and using multi scale analysis to compute a feature vector around it. Good results were obtained using an artificial scenario created by randomly rotating one image per user for different users. The dataset size is 60 images, rotated 5 times each. The performance of the system is about a 99% accuracy. However, the experimental results do not offer error measures in a real-case scenario where different images from the same individual are compared.

Based on the idea of fingerprint minutiae [4, 16], a robust pattern was first introduced in [17] where a set of landmarks (bifurcations and crossovers of retinal vessel tree) were extracted and used as feature points. In this scenario, the pattern matching problem is reduced to a point pattern matching problem and the similarity metric has to be defined in terms of matched points. A common problem in previous approaches is that the optic disc is used as a reference structure in the image. The detection of the optic disc is a complex problem and in some individuals with eye diseases this cannot be achieved correctly. In this work, the use of reference structures is avoided to allow the system to cope with a wider range of images and users.

The paper is organised as follows: in Section 2 a description of the authentication system is presented, specially the feature points extraction and the matching stages. Section 3 deals with the analysis of some similarity metrics. Section 4 shows the effectiveness results obtained by the previously described metrics running a test images set. Finally, Section 5 provides some discussion and conclusions.

2. Authentication System Process

In this work, the retinal vessel pattern for every person is ultimately defined by a set of landmarks, or feature points, in the vessel tree. For the system to perform properly, a good representation of the retinal vessel tree is needed. The extraction of the retinal vessel tree is explained in Section 2.1. Next, the biometric pattern for an individual is obtained via the feature points extracted from the vessel tree (Section 2.2). The last stage in the authentication process is the matching between the reference stored pattern for an individual and the pattern from the acquired image (Section 2.3).

2.1. Retinal Vessel Tree Extraction. Following the idea that vessels can be thought of as creases (ridges or valleys) when images are seen as landscapes (Figure 1), curvature level curves are employed to calculate the creases (crest and valley lines).

Among the many definitions of a crease, the one based on level set extrinsic curvature or LSEC, (1), has useful invariance properties. Given a function $L : \mathbb{R}^d \to \mathbb{R}$, the level set for a constant l consists of the set of points $\{\mathbf{x} \mid L(\mathbf{x}) = l\}$. For $2D$ images, L can be considered as a topographic relief or landscape and the level sets as its level curves. Negative minima of the level curve curvature κ, level by level, form valley curves, and positive maxima form ridge curves:

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

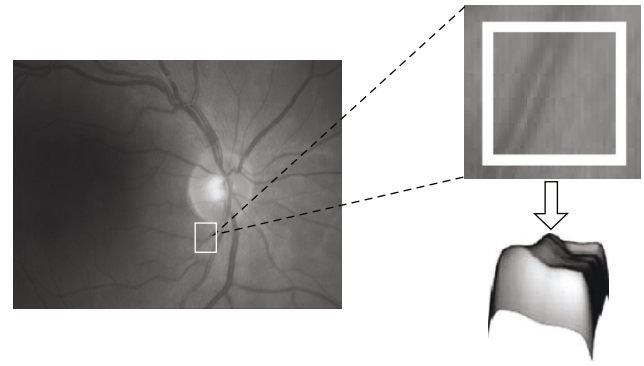


Figure 1: Representation of a region in the image as a landscape. Left side shows the retinal image with the region of interest marked with a white rectangle. In the right side, the zoomed image over the region of interest and the same region represented as a landscape, showing the creaseness feature.

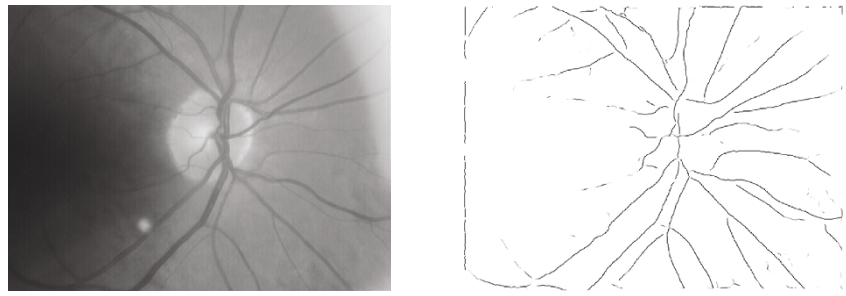
However, the usual discretization of LSEC is ill-defined in a number of cases, giving rise to unexpected discontinuities at the centre of elongated objects. Due to this, the *MLSEC-ST* operator, defined in [18, 19] for 3D landmark extraction of CT and MRI volumes, is used. This alternative definition is based on the divergence of the normalised vector field $\overline{\mathbf{w}}$:

$$\kappa = -\mathrm{div}(\overline{\mathbf{w}}). \quad (2)$$

Although (1) and (2) are equivalent in the continuous domain, in the discrete domain, when the derivatives are approximated by finite-centred differences of the Gaussian-smoothed image, (2) provides much better results. The creaseness measure κ is improved by prefiltering the image gradient vector field using a Gaussian function.

Figure 2 shows the result of the creases extraction algorithm for an input digital retinal image. Once the creases image is calculated, the retinal vessel tree is extracted and can be used as a valid biometric pattern. However, 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 and handle the whole image. To solve this, similarly to the fingerprint minutiae, a set of landmarks is extracted as the biometric pattern in the creases image. These landmarks are representative enough for each individual while consisting of a very reduced set of structures in the retinal tree. In the next subsection, the extraction process of this pattern is described.

2.2. Feature Points Extraction. The goal in this stage is to obtain a robust and consistent biometric pattern easy to



(a) (b)

Figure 2: Example of digital retinal images showing the vessel tree. (a) Input retinal image. (b) Creases image from the input representing the main vessels in the retina.

code and store. To perform this task, a set of landmarks are extracted. The most prominent landmarks in retinal vessel tree are crossovers (between two different vessels) and bifurcation points (one vessel coming out of another one) and they will be used in this work as the set of feature points constituting the biometric pattern for characterising individuals. Thus, the biometric pattern can be stored as a set of feature points.

The creases image will be used to extract the landmarks, as it is a good representation of the vessels in the retinal tree as explained earlier. The landmarks of interest are points where two different vessels are connected. Therefore, it is necessary to study the existing relationships between vessels in the image. The first step is to track and label the vessels to be able to establish those relationships between them.

In Figure 3, it can be observed that creases images show discontinuities in the crossovers and bifurcations points. This occurs because of the two different vessels (valleys or ridges) coming together into a region where the crease direction cannot be set. Moreover, due to some illumination or intensity loss issues, creases images can also show some discontinuities along a vessel (Figure 3). This issue require a process of joining segments to build the whole vessels prior to the bifurcation/crossover analysis.

Once the relationships between segments are established, a final stage will take place to remove some possible spurious feature points. Thus, the four main stages in the feature points extraction process are

(1) labelling of the vessels segments,

(2) establishing the joint or union relationships between vessels,

(3) establishing crossover and bifurcation relationships between vessels,

(4) filtering of the crossovers and bifurcations.

2.2.1. Tracking and Labelling of Vessel Segments. To detect and label the vessel segments, an image-tracking process is performed. As the creases images eliminate background information, any nonnull pixel (intensity greater than zero) belongs to a vessel segment. Taking this into account, each row in the image is tracked (from top to bottom) and when a nonnull pixel is found, the segment tracking process takes place. The aim is to label the vessel segment found, as a line of 1 pixel width. That is, every pixel will have only two neighbours (previous and next) avoiding ambiguity to track the resulting segment in further processes.

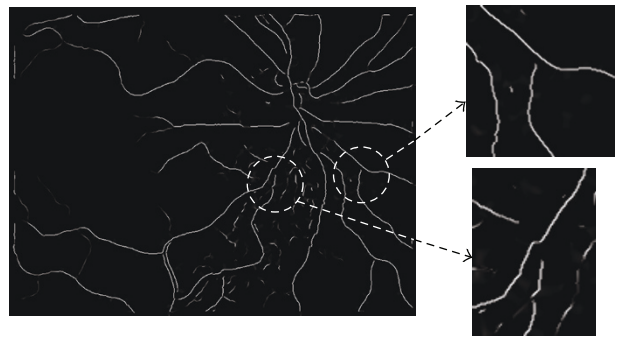


Figure 3: Example of discontinuities in the creases of the retinal vessels. Discontinuities in bifurcations and crossovers are due to two creases with different directions joining in the same region. Also, some other discontinuities along a vessel can happen due to illumination and contrast variations in the image.

To start the tracking process, the configuration of the 4 pixels which have not been analysed by the initially detected pixel is calculated. This leads to 16 possible configurations depending on whether there is a segment pixel or not in each one of the 4 positions. If the initial pixel has no neighbours, it is discarded and the image tracking continues. In the other cases there are two main possibilities: either the initial pixel is an endpoint for the segment, and this is tracked in one way only or the initial pixel is a middle point and the segment is tracked in two ways from it. Figure 4 shows the 16 possible neighbourhood configurations and how the tracking directions are established in any case.

Once the segment tracking process has started, in every step a neighbour of the last pixel flagged as segment is chosen to be the next. This choice is made using the following criterion: the best neighbour is the one with most nonflagged yet neighbours belonging to the segment. This heuristic contains the idea of keeping the 1pixel width segment to track along the middle of the crease (where pixels have more segment pixels neighbours), keeping also

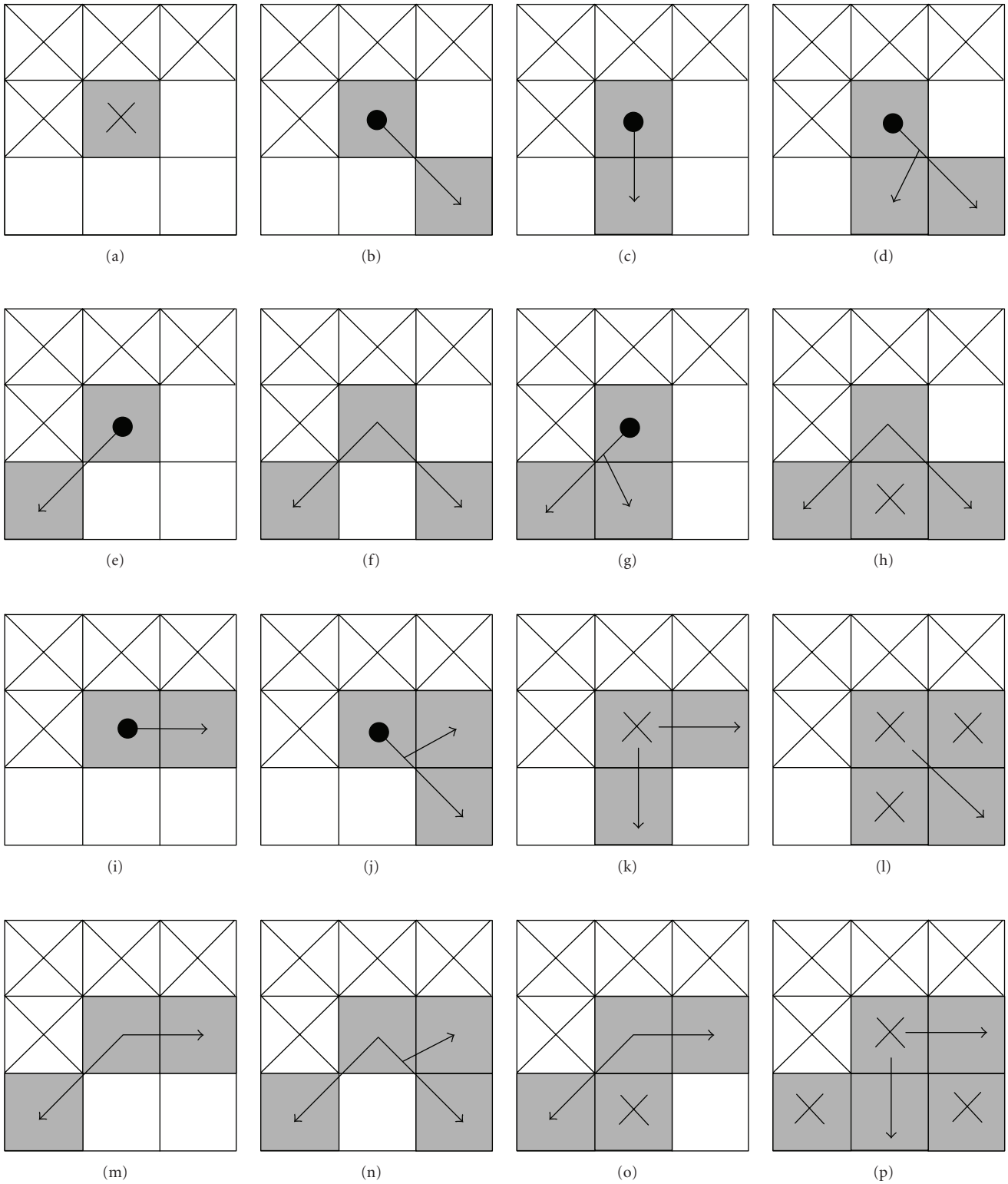


Figure 4: Initial tracking process for a segment depending on the neighbours pixels surrounding the first pixel found for the new segment in a 8-neighbourhood. As there are 4 neighbours not tracked yet (the bottom row and the one to the right), there are a total of 16 possible configurations. Gray squares represent crease (vessel) pixels and white ones background pixels. The upper row neighbours and the left one are ignored as they have already been tracked due to the image tracking direction. Arrows point to the next pixels to track while crosses flag pixels to be ignored. In (d), (g), (j) and (n) the forked arrows mean that only the best of the pointed pixels (i.e., the one with more new vessel pixels neighbours) is selected for continuing the tracking. Arrows starting with a black circle flag the central pixel as an endpoint for the segment ((b), (c), (d), (e), (g), (i), (j)).

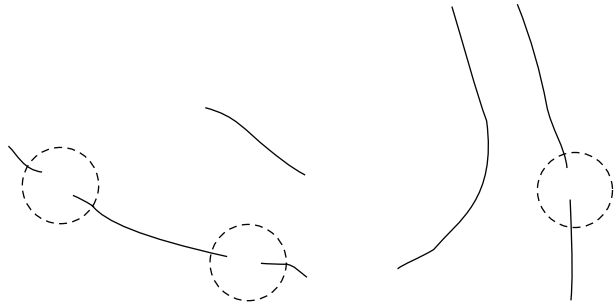


Figure 5: Examples of union relationships. Some of the vessels present discontinuities leading to different segments. These discontinuities are detected in the union relationships detection process.

the original orientations in every step. When the whole image tracking process finishes, every segment is a 1pixel-width line with its endpoints defined. The endpoints are very useful to establish relationships between segments as those relationships can always be detected in the surroundings of a segment endpoint. This avoids the analysis of every pixel belonging to a vessel, considerably reducing the complexity of the algorithm and, therefore, the running time. Finally, to avoid some spurious segments or noise to appear, small segments are removed using a length threshold.

2.2.2. Union Relationships. As stated before, unions detection is needed to build the vessels out of their segments. Aside the segments from the creases image, no additional information is required and therefore is the first kind of relationship to be detected in the image. An union or joint between two segments exists when one of the segments is the continuation of the other in the same retinal vessel. Figure 5 shows some examples of union relationships between segments.

To find these relationships, the developed algorithm uses the segment endpoints calculated and labelled in the previous subsection. The main idea is to analyse pairs of close endpoints from different segments and quantify the likelihood of one being the prolongation of the other. The proposed algorithm connects both endpoints and measures the smoothness of the connection.

An efficient approach to connect the segments is using a straight line between both endpoints. In Figure 6(a), a graphical description of the detection process for an union is showed. The smoothness measurement is obtained from the angles between the straight line and the segment direction. The segment direction is calculated by the endpoint direction. The maximum smoothness occurs when both angles are π rad., that is, both segments are parallel and belong to the straight line connecting it. The smoothness decreases as both angles decrease. A criterion to accept the candidate relationship must be established. A minimum angle $\theta_{\min}$ is set as the threshold for both angles. This way, the criterion to accept an union relationship is defined as

$$\text{Union}(r,s) = (\alpha > \theta_{\min}) \wedge (\beta > \theta_{\min}), \tag{3}$$

where r, s are the segments involved in the union and α, β their respective endpoints directions. It has been observed that for values of $\theta_{\min}$ close to $(3/4)\pi$ rad. the algorithm delivers good results in all cases.

2.2.3. Bifurcation/Crossover Relationships. Bifurcations and crossovers are the feature interest points in this work for characterising individuals by a biometric pattern. A crossover is an intersection between two segments. A bifurcation is a point in a segment where another one starts from. While unions allow to build the vessels, bifurcations allow to build the vessel tree by establishing relationships between them. Using both types the retinal vessel tree can be reconstructed by joining all segments. An example of this is shown in Figure 6(b).

A crossover can be seen in the segments image, as two bifurcations between a segment and two others related by an union. Therefore, finding bifurcation and crossover relationships between segments can be reduced to find only bifurcations. Crossovers can then be detected analysing close bifurcations.

In order to find bifurcations in the image, an idea similar to the union algorithm is followed: search the bifurcations from the segments endpoints. The criterion in this case is finding a segment close to an endpoint whose segment can be assumed to start in the found one. This way, the algorithm does not require to track the whole segments, bounding complexity to the number of segments and not to their length.

For every endpoint in the image, the process is as follows (Figure 6(c)):

(1) compute the endpoint direction,

(2) extend the segment in that direction a fixed length $l_{\max}$,

(3) analyse the points in and nearby the prolongation segment to find candidate segments,

(4) if a point of a different segment is found, compute the angle (α) associated to that bifurcation, defined by the direction of this point and the extreme direction from step 1.

To avoid undefined prolongation of the segments, a new parameter $l_{\max}$ is inserted in the model. If it follows that $l \leq l_{\max}$, the segments will be joined and a bifurcation will be detected, being l the distance from the endpoint of the segment to the other segment.

Figure 7 shows one example of results after this stage. Feature points are marked. Also, spurious detected points are identified in the image. These spurious points may occur for different reasons such as wrongly detected segments. In the image test set used (over 100 images) the approximate mean number of feature points detected per image was 28. The mean of spurious points corresponded to 5 points per image. To improve the performance of the matching process is convenient to eliminate as spurious points as possible. Thus, the last stage in the biometric pattern extraction process will be the filtering of spurious points in order to obtain an accurate biometric pattern for an individual.

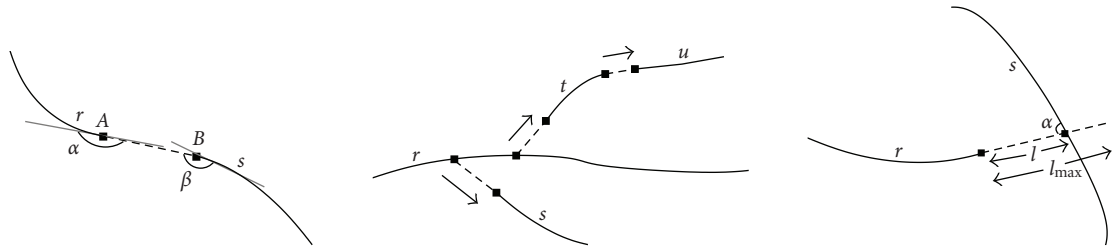


Figure 6: (a) Union of creases segments r and s. The angles between the new segment $\overline{AB}$ and the creases segments r (α) and s (β) are near π rad. so they are above the required threshold ($(3/4)\pi$) and the union is finally accepted. (b) Retinal Vessel Tree reconstruction by unions (t, u) and bifurcations (r, s) and (r, t). (c) Bifurcation between segment r and s. The endpoint of r is prolonged a maximum distance $l_{\max}$ and eventually a point of segment s is found.

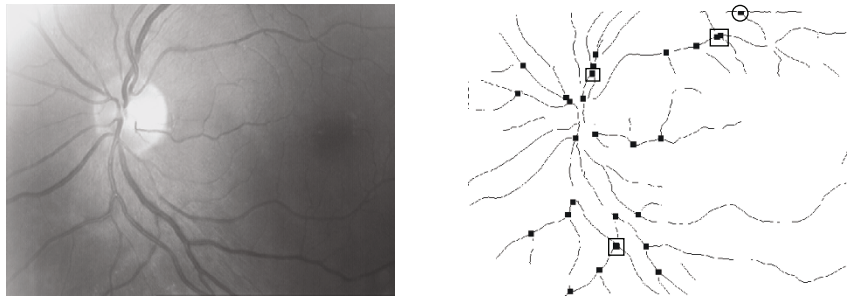


Figure 7: Example of feature points extracted from original image after the bifurcation/crossover stage. (a) Original Image. (b) Feature points marked over the segment image. Spurious points are signalled. Circles surrounding spurious points due to false segments extracted from the image borders and squares surrounding pairs of points corresponding to the same crossover (detected as two bifurcations).

2.2.4. Filtering of Feature Points. As showed in Figure 7(b), the highest feature point detected comes from a bifurcation involving an spurious segment. This segment appears in the creases extraction stage as this algorithm can make some false creases to appear in the image borders.

To avoid these situations, feature points very close to image borders are removed as the vast majority of them correspond to bifurcations involving false segments. A minimum distance to the border threshold of approximately 3% of the width/height of the image is enough to avoid these false features.

A segment filtering process takes place in the tracking stage, filtering detected segments by their length. This leads to images with minimum false segments and with only important segments in the vessel tree.

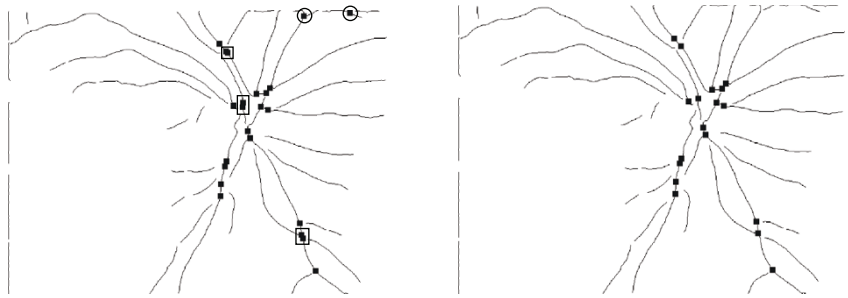
Finally, as crossover points are detected as two bifurcation points, Figure 7(b), these are merged into an unique feature point.

Figure 8 shows an example of the filtering process result, that is, the biometric pattern obtained from an individual. In resume, the average of 5 spurious points per image was reduced to 2 per image after the filtering process. These points are derived from bad extracted regions in the creases stage. The removal of non spurious points with this technique is almost null (around 0.2 points per image in the average).

2.3. Biometric Pattern Matching. In the matching stage, the stored reference pattern, ν, for the claimed identity is compared to the pattern extracted, ν', during the previous stage. Due to the eye movement during the image acquisition stage, it is necessary to align β with α in order to be matched [20–22]. This fact is illustrated in Figure 9 where two images from the same individual, Figures 9(a) and 9(c), and the obtained results in each case, Figures 9(b) and 9(d), are showed.

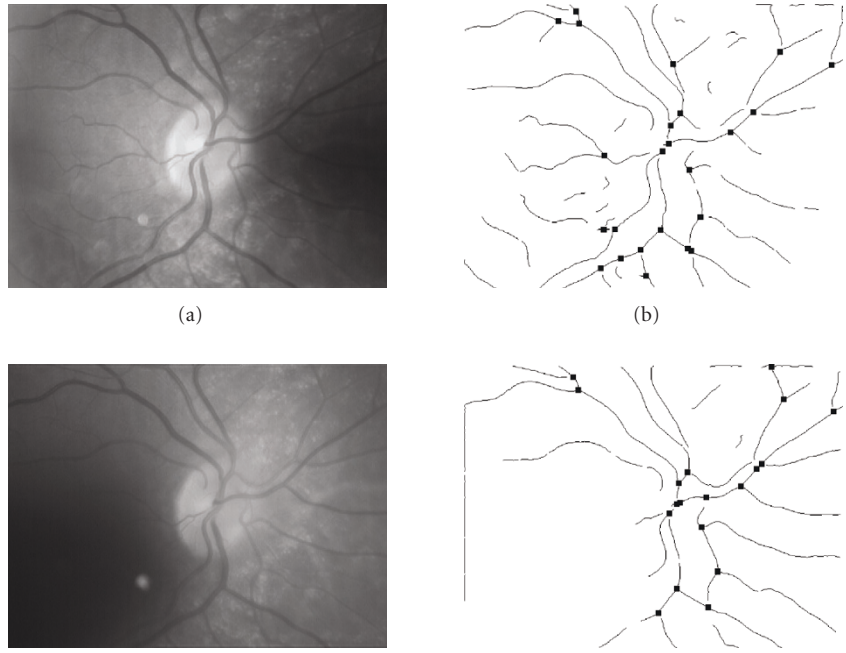
Depending on several factors, such as the eye location in the objective, patterns may suffer some deformations. A reliable and efficient model is necessary to deal with these deformations allowing to transform the candidate pattern in order to get a pattern similar to the reference one. The movement of the eye in the image acquisition process basically consists in translation in both axis, rotation and sometimes a very small change in scale. It is also important to note that both patterns ν and ν' could have a different number of points as seen in Figure 9 where, from the same individual, two patterns are extracted with 24 and 19 points. This is due to the different conditions of illumination and orientation in the image acquisition stage.

The transformation considered in this work is the similarity transformation (ST), which is a special case of the global affine transformation (GAT). ST can model translation, rotation and isotropic scaling using 4 parameters



(a) (b)

Figure 8: Example of the result after the feature points filtering. (a) Image containing feature points before filtering. (b) Image containing feature points after filtering. Spurious points from image borders and duplicate crossover points have been eliminated.



(a) (b)

(c) (d)

Figure 9: Examples of feature points obtained from images of the same individual acquired in different times. (a) (c) Original images. (b) Feature points image from (a). A total of 24 points are obtained. (d) Feature points image from (c). A total of 19 points are obtained.

[23]. The ST works fine with this kind of images as the rotation angle is moderate. It has also been observed that the scaling, due to eye proximity to the camera, is nearly constant for all the images. Also, the rotations are very slight as the eye orientation when facing the camera is very similar. Under these circumstances, the ST model appears to be very suitable.

The ultimate goal is to achieve a final value indicating the similarity between the two feature points set, in order to decide about the acceptance or the rejection of the hypothesis that both images correspond to the same individual. To develop this task the matching pairings between both images must be determined. A transformation has to be applied to the candidate image in order to register its feature points with respect to the corresponding points in the reference image. The set of possible transformations is built based on some restrictions and a matching process is performed for each one of these. The transformation with the highest matching score will be accepted as the best transformation.

To obtain the four parameters of a concrete ST, two pairs of feature points between the reference and candidate patterns are considered. If M is the total number of feature points in the reference pattern and N the total number of points in the candidate one, the size of the set T of possible transformations is computed using (4):

$$T = \frac{(M^2 - M)(N^2 - N)}{2}, \tag{4}$$

where M and N represent the cardinality of ν and ν', respectively.

Since T represents a high number of transformations, some restrictions must be applied in order to reduce it. As

the scale factor between patterns is always very small in this acquisition process, a constraint can be set to the pairs of points to be associated. In this scenario, the distance between both points in each pattern has to be very similar. As it cannot be assumed that it will be the same, two thresholds are defined, $S_{\min}$ and $S_{\max}$, to bound the scale factor. This way, elements from T are removed where the scale factor is greater or lower than the respective thresholds $S_{\min}$ and $S_{\max}$. However, (5) formalises this restriction:

$$S_{\min} < \frac{\text{distance}(p,q)}{\text{distance}(p',q')} < S_{\max}, \tag{5}$$

where p, q are points from ν pattern, and p', q' are the matched points from the ν pattern. Using this technique, the number of possible matches greatly decrease and, in consequence, the set of possible transformations decreases accordingly. The mean percentage of not considered transformations by these restrictions is around 70%.

In order to check feature points, a similarity value between points (SIM) is defined which indicates how similar two points are. The distance between these two points will be used to compute that value. For two points A and B, their similarity value is defined by

$$\text{SIM}(A,B) = 1 - \frac{\text{distance}(A,B)}{D_{\max}}, \tag{6}$$

where $D_{\max}$ is a threshold that stands for the maximum distance allowed for those points to be considered a possible match. If $\text{distance}(A,B) > D_{\max}$, then $\text{SIM}(A,B) = 0$. $D_{\max}$ is a threshold introduced in order to consider the quality loss and discontinuities during the creases extraction process leading to mislocation of feature points by some pixels.

In some cases, two points B_1, B_2 could have both a good value of similarity with one point A in the reference pattern. This happens because B_1 and B_2 are close to each other in the candidate pattern. To identify the most suitable matching pair, the possibility of correspondence is defined comparing the similarity value between those points to the rest of similarity values of each one of them:

$$P(A_i,B_j) = \frac{\text{SIM}(A_i,B_j)^2}{\left(\sum_{i'=1}^{M}\text{SIM}(A_{i'},B_j)+\sum_{j'=1}^{N}\text{SIM}(A_i,B_{j'})-\text{SIM}(A_i,B_j)\right)}. \tag{7}$$

An $M \times N$ matrix Q is constructed such that position (i,j) holds $P(A_i,B_j)$. Note that if the similarity value is 0, the possibility value is also 0. This means that only valid matchings will have a non-zero value in Q. The desired set C of matching feature points is obtained from P using a greedy algorithm. The element (i,j) inserted in C is the position in Q where the maximum value is stored. Then, to prevent the selection of the same point in one of the images again, the row (i) and the column(j) associated to that pair are set to 0. The algorithm finishes when no more non-zero elements can be selected from Q.

The final set of matched points between patterns is C. Using this information, a similarity metric must be established to obtain a final criterion of comparison between patterns. Performance of several metrics using matched points information is analysed in Section 3.

3. Similarity Metrics Analysis

The goal in this stage of the process is to define similarity measures on the aligned patterns to correctly classify authentications in both classes: attacks (unauthorised accesses), when the two matched patterns are from different individuals and clients (authorised 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 [24] were used. The rest of the images will be used for testing in Section 4. The images from the database have been acquired with a TopCon nonmydriatic camera NW-100 model and are optic disc centred with a resolution of 768×584. There are 60 individuals with two or more images acquired in a time span of 6 years. 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 150×150 matchings) for each metric. The matchings are classified into attacks or clients accesses depending if the images belong to the same individual or not. Distributions of similarity values for both classes are compared in order to analyse the classification capabilities of the metrics.

The main information to measure similarity between two patterns is the number of feature points successfully matched between them. Figure 10(a) shows the 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 overlapping between them.

This overlapping is caused by the variability of the patterns size in the training set because of the different illumination and contrast conditions in the acquisition stage. Figure 10(b) shows the histogram for the biometric pattern size, that is, the number of feature points detected. A high variability can be observed, as some patterns have more than twice the number of feature points of other patterns. As a result of this, some patterns have a small size, capping the possible number of matched points (Figure 11). Also, using the matched points information alone lacks a well bounded and normalised metric space.

To combine information of patterns size and normalise the metric, a function f will be used. Normalised metrics are very common as they make easier to compare class separability or establishing valid thresholds [25]. The similarity measure (S) between two patterns will be defined by

$$S = \frac{C}{f(M,N)}, \tag{8}$$

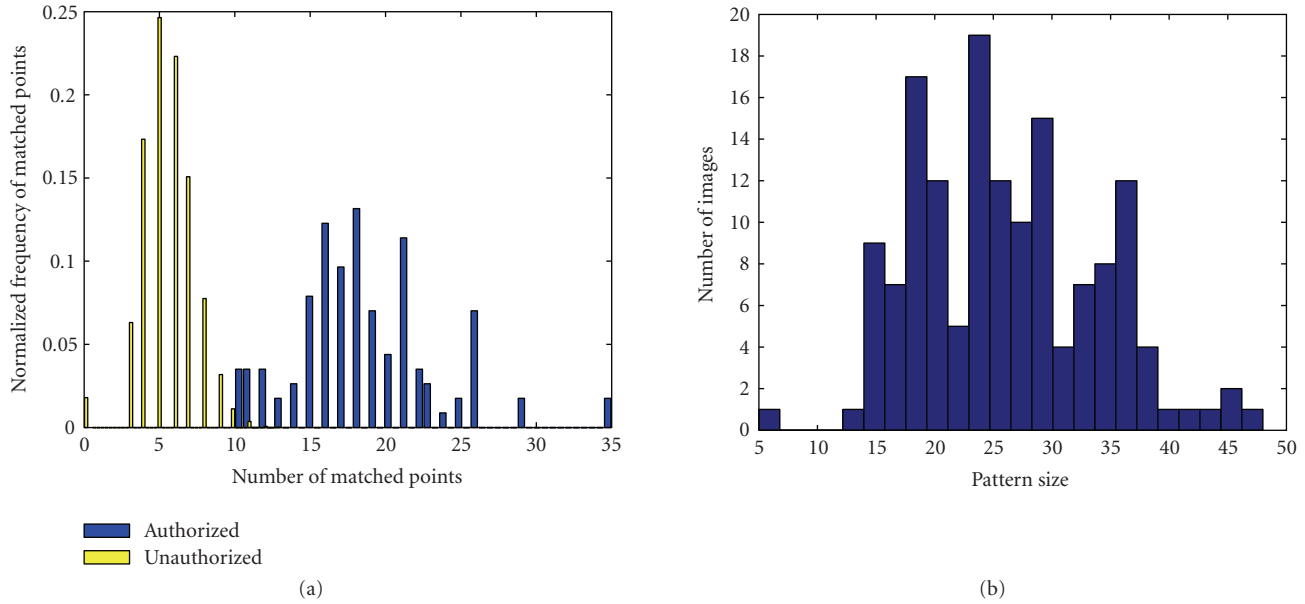


Figure 10: (a) Matched points histogram in the attacks (unauthorised) and clients (authorised) authentications cases. In the interval [10, 13] both distributions overlap. (b) histogram of detected points for the patterns extracted from the training set.

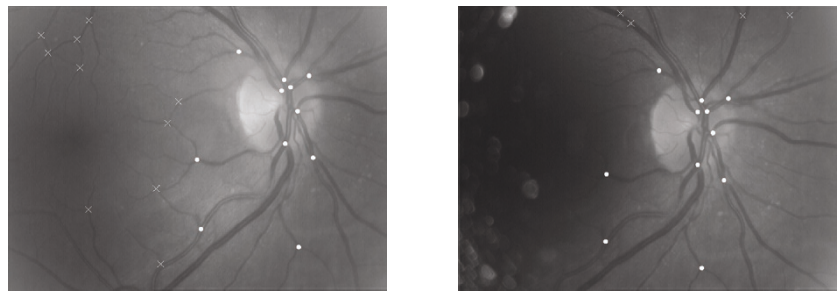


Figure 11: Example of matching between two samples from the same individual in VARIA database. White circles mark the matched points between both images while crosses mark the unmatched points. In (b) the illumination conditions of the image lead to miss some features from left region of the image. Therefore, a small amount of detected feature points is obtained capping the total amount of matched points.

where C is the number of matched points between patterns, and M and N are the matching patterns sizes. The first f function defined and tested is:

$$f(M,N) = \min(M,N). \tag{9}$$

The min function is the less conservative one as it allows to obtain a maximum similarity even in cases of different sized patterns. Figure 12(a) shows the distributions of similarity scores for clients and attacks classes in the training set using the normalisation function defined in (9), and Figure 12(b) shows the FAR and FRR curves versus the decision threshold.

Although the results are good when using the normalisation function defined in (9), a few cases of attacks show high similarity values, overlapping with the clients class. This is caused by matchings involving patterns with a low number of feature points as $\min(M,N)$ will be very small, needing only a few points to match in order to get a high similarity value. This suggests, as it will be reviewed in Section 4, that some minimum quality constraint in terms of detected points would improve performance for this metric.

To improve the class separability, a new normalisation function f is defined:

$$f(M,N) = \sqrt{MN}. \tag{10}$$

Figure 13(a) shows the distributions of similarity scores for clients and attacks classes in the training set using the normalisation function defined in (10) and Figure 13(b) shows the FAR and FRR curves versus the decision threshold.

Function defined in (10) combines both pattern sizes in a more conservative way, preventing the system to obtain a high similarity value if one pattern in the matching process contains a low number of points. This allows to reduce the attacks class variability and, moreover, to separate its values away from the clients class as this class remains in a similar values range. As a result of the new attacks class boundaries,

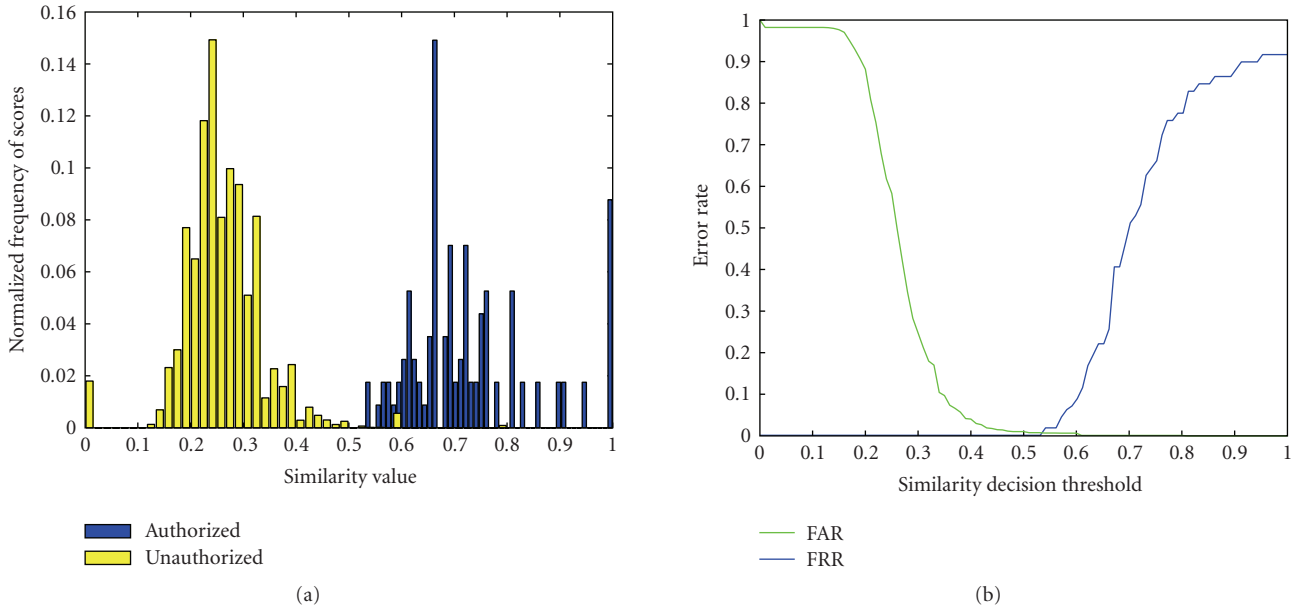


Figure 12: (a) Similarity values distribution for authorised and unauthorised accesses using $f = \min(M, N)$ as normalisation function for the metric. (b) False accept rate (FAR) and false rejection rate (FRR) for the same metric.

a decision threshold can be safely established where FAR = FRR = 0 in the interval $[0.38, 0.5]$ as Figure 13(b) clearly exposes. Although this metric shows good results, it also has some issues due to the normalisation process which can be corrected to improve the results as showed in next subsection.

3.1. Confidence Band Improvement. Normalising the metric has the side effect of reducing the similarity between patterns of the same individual where one of them had a much greater number of points than the other, even in cases with a high number of matched points. This means that some cases easily distinguishable based on the number of matched points are now near the confidence band borders. To take a closer look at this region surrounding the confidence band, the cases of unauthorised accesses with the highest similarity values (S) and authorised accesses with the lowest ones are evaluated. Figure 14 shows the histogram of matched points for cases in the marked region of Figure 13(b). It can be observed that there is an overlapping but both histograms are highly distinguishable.

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. The new metric is defined as

$$S_\gamma = S \cdot C^{\gamma-1} = \frac{C^\gamma}{\sqrt{MN}} \tag{11}$$

with S, C, M, and N the same parameters from (10). The γ correction parameter allows to improve the similarity values when a high number of matched points is obtained, specially in cases of patterns with a high number of points.

Using the gamma parameter, values can be higher than 1. In order to normalise the metric back into a $[0, 1]$ values space, a sigmoid transference function, $T(x)$, is used:

$$T(x) = \frac{1}{1 + e^{s\cdot(x-0.5)}}, \tag{12}$$

where s is a scale factor to adjust the function to the correct domain as S_γ does not return negatives or much higher than 1 values when a typical $\gamma \in [1, 2]$ is used. In this work, $s = 6$ was chosen empirically. The normalised gamma-corrected metric, $S'_\gamma(x)$, is defined by

$$S'_\gamma = T(S_\gamma). \tag{13}$$

Finally, to choose a good γ parameter, the confidence band improvement has been evaluated for different values of γ (Figure 15(a)). The maximum improvement is achieved at $\gamma = 1.12$ with a confidence band of 0.3288, much higher than the original from previous section. The distribution of the whole training set (using $\gamma = 1.12$) is showed in Figure 15(b) where the wide separation between classes can be observed.

4. Results

A set of 90 images, 83 different from the training set, and 7 from the previous set with the highest number of points, has been built in order to test the metrics performance once their parameters have been fixed with the training set. To test the metrics performance, the false acceptance rate and false rejection rate were calculated for each of them (the metrics normalised by (9), (10) and the gamma-corrected normalised metric defined in (13).

A usual error measure is the equal error rate (EER) that indicates the error rate where FAR curve and FRR curve

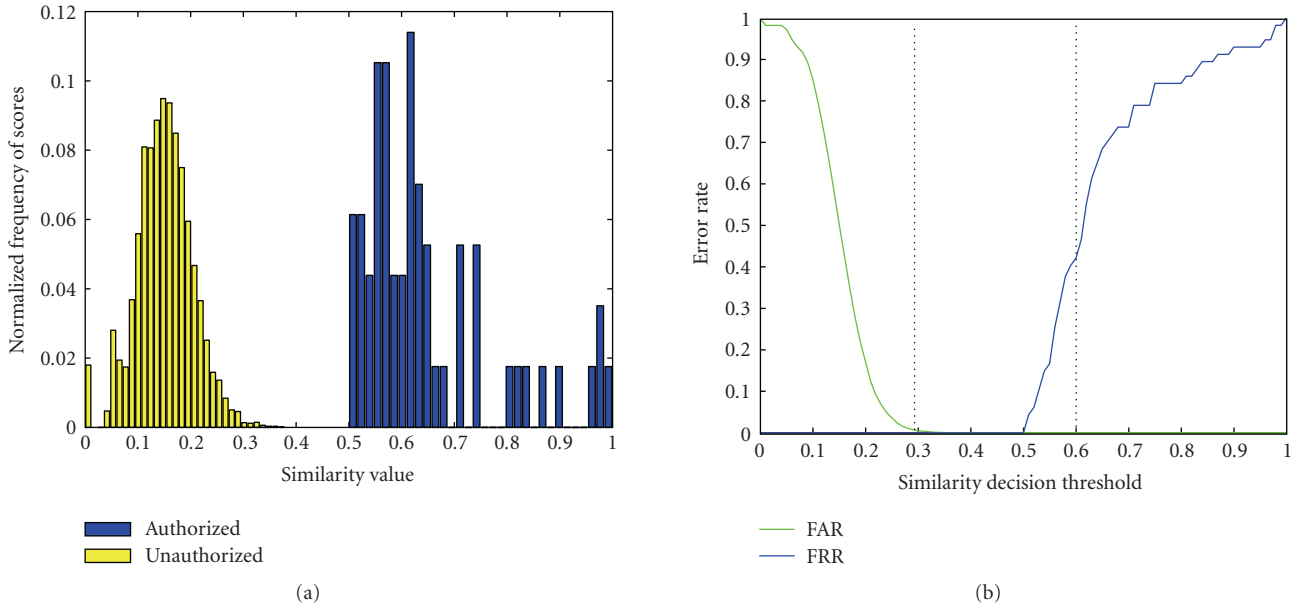


Figure 13: (a) Similarity values distribution for authorised and unauthorised accesses using $f = \sqrt{MN}$ as normalisation function for the metric. (b) False accept rate (FAR) and false rejection rate (FRR) for the same metric. Dotted lines delimit the interest zone surrounding the confidence band which will be used for further analysis.

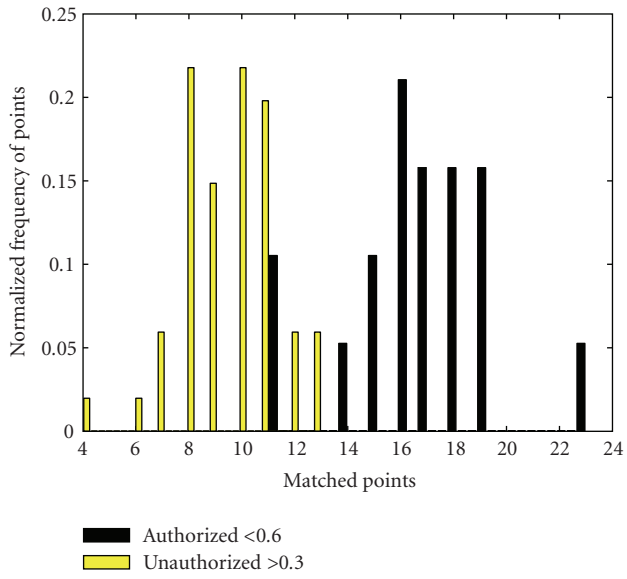


Figure 14: Histogram of matched points in the populations of attacks whose similarity is higher than 0.3 and clients accesses whose similarity is lower than 0.6.

intersect. Figure 16(a) shows the FAR and FRR curves for the three previously specified metrics. The EER is 0 for the normalised by geometrical mean (mean) and gamma corrected (gamma) 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 0.2337.

The establishment of a wide confidence band is specially important in this scenario of different images from users acquired on different times and with different configurations of the capture hardware.

Finally, to evaluate the influence of the image quality, 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 16(b) 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, 25.2, the confidence band grows from 0.2337 to 0.3317. So removing half of the images, the band is increased only by 0.098 suggesting that the gamma-corrected metric is very robust to low quality images.

The mean execution time on a 2.4 Ghz. Intel Core Duo desktop PC for the authentication process, implemented in C++, was 155 milliseconds: 105 milliseconds in the feature extraction stage and 50 milliseconds in the registration and similarity measure estimation, so that the method is very well fitted to be employed in a real verification system.

5. Conclusions and Future Work

In this work, a complete identity verification method has been introduced. Following the same idea as the fingerprint minutiae-based methods, a set of feature points is extracted from digital retinal images. This unique pattern will allow for the reliable authentication of authorised users. To get the set of feature points, a creases-based extraction algorithm is used. After that, a recursive algorithm gets the point features by tracking the creases from the localised optic disc. Finally, a registration process is necessary in order

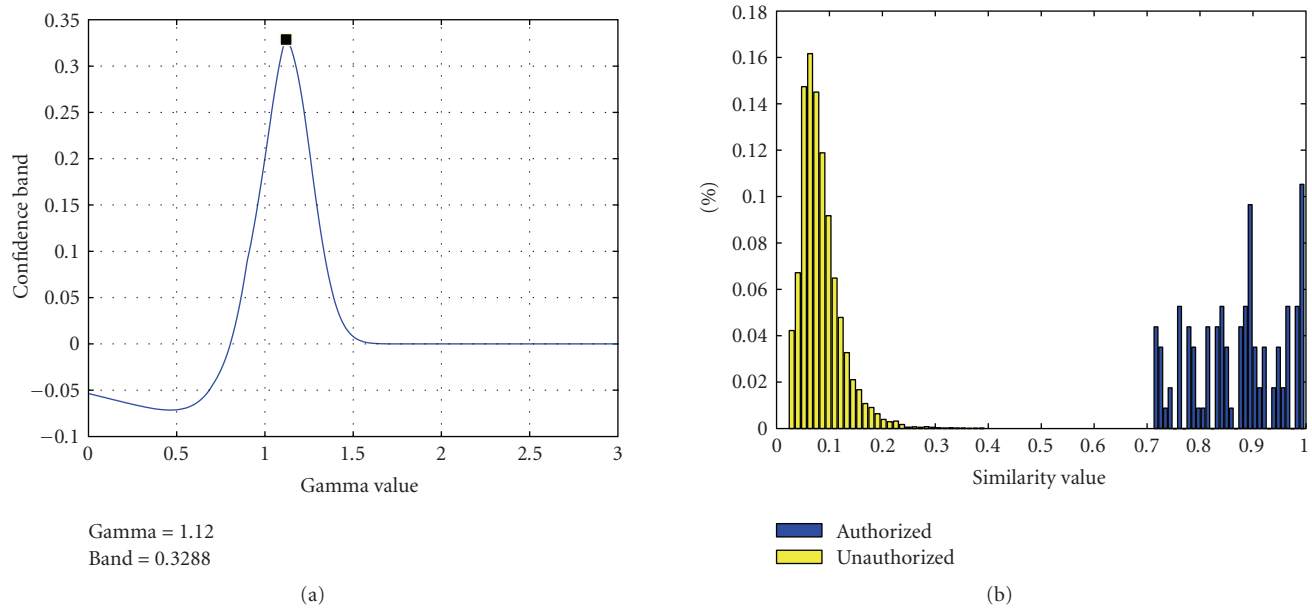


Figure 15: (a) Confidence band size versus gamma (γ) parameter value. Maximum band is obtained at $\gamma = 1.12$. (b) Similarity values distributions using the normalised metric with $\gamma = 1.12$.

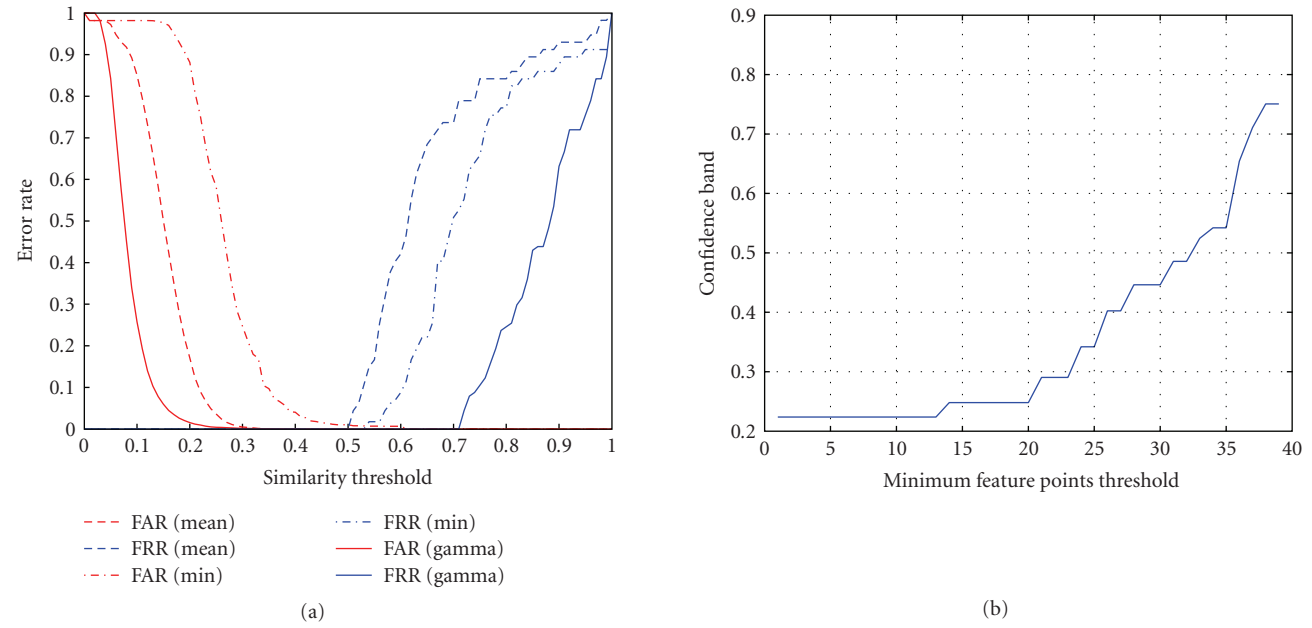


Figure 16: (a) FAR and FRR curves for the normalised similarity metrics (min: normalised by minimum points, mean: normalised by geometrical mean, and gamma: gamma corrected metric). The best confidence band is the one belonging to the gamma corrected metric corresponding to 0.2337.(b) Evolution of the confidence band using a threshold of minimum detected points per pattern.

to match the reference pattern from the database and the acquired one. With the patterns aligned, it is possible to measure the degree of similarity by means of a similarity metric. Normalised metrics have been defined and analysed in order to test the classification capabilities of the system. 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 individuals is a robust biometric pattern allowing to define metrics that offer a good confidence band even in unconstrained environments when the image quality variance can be very high in terms of distortion, illumination, or definition. This is also possible as this methodology does not rely on the localisation or segmentation of some reference structures, as it might be the optic disc. Thus, if the the user suffers some structure-distorting pathology and this structure cannot be detected,

the system works the same with the only problem being a possible loss of feature points constrained to that region.

Future work includes the use of some high-level information of points to complement metrics performance and new ways of codification of the biometric pattern allowing to perform faster matches.

Acknowledgment

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

References

[1] J. G. Daugman, "Biometric personal identification system based on iris analysis," US patent no. 5291560, 1994.

[2] Retica Systems, "Iris-Retinal multimodal identification," http://www.retica.com/site/technology/irisretina.html.

[3] Digital Persona, "Fingerprint solutions," http://www.digitalpersona.com/index.php.

[4] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1365–1388, 1997.

[5] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 1, pp. 3–18, 2006.

[6] R. Zunkel, "Hand geometry based verification," in *BIOMETRICS: Personal Identification in Networked Society*, pp. 87–101, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999.

[7] W. Zhao, R. Chellappa, A. Rosenfeld, and P. Phillips, "Face recognition: a literature survey," Tech. Rep., National Institute of Standards and Technology, Gaithersburg, Md, USA, 2000.

[8] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: a survey," *Pattern Recognition Letters*, vol. 28, no. 14, pp. 1885–1906, 2007.

[9] J. Bigun, C. Chollet, and G. Borgefors, Eds., *Proceedings of the 1st International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '97)*, Crans-Montana, Switzerland, March 1997.

[10] L. Ballard, D. Lopresti, and F. Monrose, "Forgery quality and its implications for behavioral biometric security," *IEEE Transactions on Systems, Man, and Cybernetics Part B*, vol. 37, no. 5, pp. 1107–1118, 2007.

[11] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, 2007.

[12] S. C. Dass, Y. Zhu, and A. K. Jain, "Validating a biometric authentication system: sample size requirements," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1902–1913, 2006.

[13] C. Mariño, M. G. Penedo, M. Penas, M. J. Carreira, and F. González, "Personal authentication using digital retinal images," *Pattern Analysis and Applications*, vol. 9, no. 1, pp. 21–33, 2006.

[14] C. Mariño, M. G. Penedo, M. J. Carreira, and F. González, "Retinal angiography based authentication," in *Proceedings of the 8th Iberoamerican Congress on Pattern Recognition (CIARP '03)*, vol. 2905 of *Lecture Notes in Computer Science*, pp. 306–313, Havana, Cuba, November 2003.

[15] H. Farzin, H. Abrishami-Moghaddam, and M.-S. Moin, "A novel retinal identification system," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Article ID 280635, 10 pages, 2008.

[16] X. Tan and B. Bhanu, "A robust two step approach for fingerprint identification," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2127–2134, 2003.

[17] M. Ortega, C. Mariño, M. G. Penedo, M. Blanco, and F. González, "Personal authentication based on feature extraction and optic nerve location in digital retinal images," *WSEAS Transactions on Computers*, vol. 5, no. 6, pp. 1169–1176, 2006.

[18] A. M. López, D. Lloret, J. Serrat, and J. J. Villanueva, "Multilocal creaseness based on the level-set extrinsic curvature," *Computer Vision and Image Understanding*, vol. 77, no. 2, pp. 111–144, 2000.

[19] A. M. Löpez, F. Lumbreras, J. Serrât, and J. J. Villanueva, "Evaluation of methods for ridge and valley detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 21, no. 4, pp. 327–335, 1999.

[20] L. G. Brown, "A survey of image registration techniques," *ACM Computing Surveys*, vol. 24, no. 4, pp. 325–376, 1992.

[21] B. Zitová and J. Flusser, "Image registration methods: a survey," *Image and Vision Computing*, vol. 21, no. 11, pp. 977–1000, 2003.

[22] M. S. Markov, H. G. Rylander III, and A. J. Welch, "Real-time algorithm for retinal tracking," *IEEE Transactions on Biomedical Engineering*, vol. 40, no. 12, pp. 1269–1281, 1993.

[23] N. Ryan, C. Heneghan, and P. de Chazal, "Registration of digital retinal images using landmark correspondence by expectation maximization," *Image and Vision Computing*, vol. 22, no. 11, pp. 883–898, 2004.

[24] VARIA, "VARPA Retinal images for authentication," http://www.varpa.es/varia.html.

[25] M. Tico and P. Kuosmanen, "Fingerprint matching using an orientation-based minutia descriptor," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 8, pp. 1009–1014, 2003.