# Automatic Detection of the Optimal Acceptance Threshold in a Face Verification System

Raquel Montes Diez, Cristina Conde, and Enrique Cabello

Universidad Rey Juan Carlos (ESCET),
C/Tulipán s/n,
28933 Móstoles, Spain
r.montes@escet.urjc.es
http://frav.escet.urjc.es

**Abstract.** We present a face verification system with an acceptance threshold automatically computed. The user is allowed to provide the rate between the costs assumed for a false acceptance and false rejection. This rate between costs can be intuitively known by the system responsible and are a starting point to fulfil user security requirements. With this user-friendly data, an algorithm based on screening techniques to compute the acceptance threshold is presented in this paper. This algorithm is applied to an original and competitive face verification system based on principal component analysis and two classifiers (neural network radial basis function and support vector machine). Experimental results with a 100 people face database are shown. This method can be also applied into other biometric applications in which this threshold should be calculated.

## 1 Introduction

Biometrics technology has passed in few years from research labs to commercial implementations. Media coverage has brought face recognition systems used in high profile locations such as airports, to the attention of the public. Unfortunately, the recognition of the human face is a very complex problem involving several processing steps that have not yet been completely resolved. Although technology is evolving and obtaining better results, expectations are very high and in most cases, difficult to achieve. As a consequence, several systems tested in real conditions have been rejected.

However, less attention has been paid to control access systems. In these systems, the effect of the environment is more controlled, allowing the technology to obtain better and more reliable results. Such systems could fulfil the performance criteria demanded by potential clients.

The experiment presented in this paper focused on testing the performance of a control access system based on face verification technology. In control access environments, it is possible to take advantage of a set of specific characteristics. Usually, the subject is in front of the camera, only one subject appears, the size of the face is more or less constant and the subject is usually collaborative. It is therefore possible to obtain an initial set of images and to define a personal identification

D. Maltoni and A.K. Jain (Eds.): BioAW 2004, LNCS 3087, pp. 70-79, 2004.

number entered or placed in a smart card. Our system uses these advantages and proposes a control access system designed to work in such situations.

In recent years, two main approaches to face processing problem using only image information have appeared. The first approach is Principal Components Analysis (PCA) and related methods such as Fisherfaces [1] [2] [3] [4]. These methods consider only the global information of the face. Likewise, methods based on Local Feature Analysis (LFA) [5] [6], similar to PCA, consider different kernel functions which concentrate local features, such as eyes, mouth and nose. In this case, selection of facial features and kernels is an open issue. The second approach, based on Elastic Bunch Graph Matching (EBGM) [7] and similar methods, use wavelet transformation to obtain local description of the face and a graph to obtain a global face description. In the scientific literature several results with different research algorithms have been published. For example, following the success of FERET tests [8] [9] [10], a recent and extensive test of ten commercial products has been performed (FRVT 2002) [11].

A continuing problem in the design of a facial verification system is the decision of the optimum acceptance threshold. The acceptance threshold is the value that determines whether a verification is acceptance or rejection. For example, in the SVM classifier, the threshold is $w = 0$. However our experience shows that choosing a different value could result in a better performance of the system, this is, in a smaller number of false acceptance and false rejection. We understand that the acceptance threshold should then be chosen to minimize the error rate.

Furthermore, it is important to note that in a facial verification system there are two different error types; false acceptance and a false rejection, each with, possibly, different associated risk. For instance, in high security environments it is highly recommended to minimize the false acceptance rate despite the fact that the false rejection rate could be increased (subject has to key maybe twice the code). Likewise, for the access to a non-critical place, a higher false acceptance rate could be acceptable and the false rejection rate could be lowered (impostors could be accepted but to gain access, the code only has to be typed once). In order to take this into account, we propose a classification system based on costs for false acceptance and false rejection. The exact calculation of both costs (acceptance and rejection) could be difficult to found, but the rate between this costs is easier to fix. This is the input in the algorithm proposed.

In this paper we present an innovative algorithm to calculate this optimal acceptance threshold by using economic screening techniques based on different costs for different error type.

## 2 Experimental Set Up Description

The set up has been designed and built to test the performance of the algorithm. Figure 1 shows the image acquisition set up, consisting on two diffuse light sources placed on both sides of a video camera.

In order to minimize distortions originated by changes in the lens focal length and the camera-subject distance, it is advisable to fix both in any operation environment. These requirements are easily met in any exploitation site. In our experiments a

database of 100 individuals is considered. Subjects were forced to change their pose between the acquisition of two consecutive images.

**Fig. 1.** Experimental set up showing diffuse lighting and the CCD camera.

**Fig. 2.** Examples of the Face Database

An image size is 320 x 240 pixels with face covering great part of the image (as shown in figure 2). Our face location system cropped the face to a window of 130x140 pixels. Eight images per subject were used for computing PCA matrix and training all classifiers. For tests sets, four different images per subject were considered.

## 3 Face Verification System

Face verification can be split into four processes: Face location, PCA computation, classifier design and automatic optimal threshold calculation. The first three parts require a training or parameter computation phase and once all parameters have been adjusted and classifiers trained, a normal operation phase. This fourth process will be detailed in chapter 4.

### 3.1 Face Location

In this step, the image is the input and the desired output is a window containing only the face in a standard size. The background is then eliminated to obtain a rough initial estimate of face location in the image. Subsequently, convolution with a face template is applied to obtain a more reliable and precise position of the face. Each subject in the database has their own template. The template is part of the subject's face, so convolution is more reliable where template coincides with the face in image. Initial tests suggest that one template per subject achieves better performance that one

template for the whole database. When the convolution reaches the maximum over the images, a window containing the face is extracted. The final dimension was reduced to 130 x 140 pixels. In this step all images were also converted from colour to a grey scale.

### 3.2 Principal Components Analysis Computation

Principal Components Analysis is the *de facto* standard in face verification systems. In the training phase, the problem can be resolved computing the transformation matrix using a number of eigenvectors that retains almost 100% of the initial variance. Only one PCA matrix is computed with the training face images set. In our experiment eight images per subject are considered in order to compute the PCA matrix, in our tests 150 eigenvalues were considered.

### 3.3 Verification

Two classifiers have been considered: Artificial Neural Networks: Radial Basis Function (RBF) and Support Vector Machine (SVM). In all cases, training is performed with eight images per subject (the same ones used for PCA computation). Tests were carried out using four images per subject. Training and test sets did not overlap. If the output value for SVM and RBF is large this means that confidence is high. Thus positive verification has been considered when output value is greater than the acceptance threshold. This acceptance threshold has to be set to obtain the optimum value that minimizes false acceptance rate and false rejection rate, and maximizes the correct rate. The magnitude used as threshold is different for each classifier, in case of RBF, output neuron value and SVM: function decision value

RBF has been used as an artificial neural network classifier for face verification. The initial information is a subject image and personal identification number (PIN) code. The PIN code indicates which output neuron is considered. In our experiment, Gaussian functions considered are symmetric and centred in the middle of each face subject cluster.

Support Vector Machine offers excellent results in 2-class problems. This classifier could be easily used in verification problems (recognizing one subject against rest). In our experiment a linear kernel has been considered.

## 4 Optimal Acceptance Threshold Calculation

In order to optimize the acceptance threshold, we perform a Bayesian screening approach [12] based on two variables, namely

- A binary performance variable $T$, identifying whether one image has been taken ($T = 1$) or not ($T = 0$) of a given person.
- A screening variable $X$ defining the output of a known classifier, for instance, SVM or RFB.

Since the screening variable $X$ is not perfectly correlated with the performance variable, decisions made by using the screen are prone to error (false acceptance and false rejection).

### 4.1 Economic Design of the Screen

Suppose that our screening variable $X$ is continuous and of the type *the larger the better*. That is, a large value of $X$ tends to indicate a matching image or genuine ($T = 1$), whereas a small value of $X$ is a sign of an impostor ($T = 0$).

Under such an assumption, a single-stage screen based on the screening variable, would naturally contain a cut-off point $w$, so that if $X$ is above $w$, we accept the person as genuine, and if $X$ is below $w$, we do not. Observe that if $X = w$ there is an arbitrary choice between accepting and rejecting the person. From now on and in order to be consistent, we shall accept items for which $X = w$, so that the screen is precisely defined as

- if $X \geq w$, the person is accepted.
- if $X < w$ the person is rejected.

### 4.2 Optimal Acceptance Threshold

We adopt an economic objective in which the value of the threshold $w$ is determined in order to minimize the expected total cost of the procedure. Let $c_a$ and $c_r$ be the cost paid for a false acceptation and a false rejection by the system, respectively. The expected total cost of an image being classified based on the output of a classifier system such as SVM or RBF, may be expressed as a function of $w$, so that

$$ETC(w) = c_r P(\text{wrongly reject image}) + c_a P(\text{wrongly accept image}).$$

In formal notation,

$$ETC(w) = c_r P(T = 1, X < w) + c_a P(T = 0, X \geq w),$$

which, assuming $X$ is continuous, becomes

$$ETC(w) = c_r \int_{-\infty}^{w} P(T = 1 \mid X = w) f(x)dx + c_a \int_{w}^{\infty} \left[1 - P\left(T = 1 \mid X = w\right)\right] f(x)dx,$$

where $f(x)$ is the marginal density function of the screening variable $X$.

To minimize this expected total cost for continuous $X$, we differentiate this expression with respect to $w$, and equate to zero,

$$ETC'(w) = c_r P(T = 1 \mid X = w) f(w) - c_a \left[1 - P\left(T = 1 \mid X = w\right)\right] f(w).$$

Defining

$$k = \frac{c_a}{c_a + c_r},$$

it is then straight forward to show that the equation

$$P(T=1 \mid X = w) = k, \tag{1}$$

gives the optimal value $w$ for the acceptance threshold. Note also that, by defining the rate $k$, there is no need to state the value of the costs $c_a$ and $c_r$. The user may just give the rate $k$, which should be easier that fixing the costs.

In order to identify the optimal limit for the first stage of the screen we need to solve equation (**1**) and, hence, to evaluate expressions of the form $P(T=1 \mid X = \mathrm{x})$. It is necessary, therefore, to take into account the structure defining the relationship between $X$ and $T$.

### 4.3 The Model

The structure for $(X,T)$ is usually expressed as a parametric model with unknown parameters $\boldsymbol{\theta}$. We denote the joint probability model for $(X,T)$ given $\boldsymbol{\theta}$ by $f(x,t \mid \boldsymbol{\theta})$ and try to obtain the unconditional model $f(x,t)$ by using the available information about the parameters. There are two main approaches for this purpose: the estimative or classical approach and the predictive or Bayesian approach. Here we shall adopt a Bayesian approach, as it provides a natural but also rigorous theory for combining prior and experimental information as well as for making inference.

We now propose the factorisation of the joint distribution of $(X,T)$ through the conditional model for the continuous screening variable given the value of the performance variable. We also specify the distribution of $X$ for genuine and impostor, separately, so that

$$f(x,t \mid \boldsymbol{\theta}) = f(x \mid T=1, \mu_1, \sigma_1^2)P(T=1 \mid \rho) + f(x \mid T=0, \mu_0, \sigma_0^2)P(T=0 \mid \rho),$$

where $\boldsymbol{\theta} = (\mu_1, \sigma_1^2, \mu_0, \sigma_0^2 \rho)$ and with $(\mu_1, \sigma_1^2)$, $(\mu_0, \sigma_0^2)$ and $\rho$ independent.

Remember that $T$ is a binary performance variable, taking values $T=1$ if a photograph match subject identity and $T=0$, otherwise. Its marginal distribution may, therefore, be defined by

$$P(T=1) = \rho,$$
$$P(T=0) = 1-\rho,$$

where $\rho$ is the probability of success and hence, satisfies $0 \le \rho \le 1$.

Let us then assume that variable $X$ follows a normal distribution with parameters $(\mu_1, \sigma_1^2)$ and $(\mu_0, \sigma_0^2)$ in each group, this is,

$$X \mid T = i \sim N(\mu_i, \sigma_i^2),$$

for $i = 0.1$, respectively.

Here we are interested in the conditional probability of an item with screening value $X = x$ being successful. By using Bayes theorem, this is,

$$P(T=1 \mid X=\ x,\ data) = \frac{f(x\ \mid T=1,\ data)P(T=1 \mid data)}{\sum_{i=0,1} f(x\ \mid T=i,\ data)P(T=i \mid data)}. \quad \textbf{(2)}$$

The conditional posterior predictive densities $f(x \mid T=i,\ data)$ for $i=0.1$ and the posterior predictive probability of a success $P(T=1 \mid data)$ are both developed by using the Bayesian approach, both assuming non—informative prior distribution for the unknown parameters, see, for instance [12].

The predictive posteriors of $X \mid T=i$, are found to be *Student-t* distributions with density functions,

$$f(x \mid T=i,\ data) \propto \frac{1}{\sqrt{p_i}}\left\{1+\frac{(x-\overline{x}_i)^2}{(n_i-2)p_i}\right\}^{-\frac{1}{2}(n_i-1)}$$

where $p_i=(1+n_i^{-1})s_i^2$ and where $\overline{x}_i$, $s_i$ and $n_i$ are the sample mean, sample standard deviation and sample size for each one of the two different groups, $i=0,1$, this is for genuine and impostors.

In developing the posterior probability of an image matching subject identity $P(T=1 \mid data)$, it is of interest to recognize that the number of successes $n_1$ and the number of failures $n_0$ have been chosen in advance, and that no additional information about the probability of success is therefore provided by the data. Thus we set a non informative prior for the parameter $\rho$ which results in equivalent posterior predictive probabilities for genuine and impostors, this is

$$P(T=1 \mid data) = \frac{1}{2}.$$

Once all the elements in expression (**2**) have been developed, optimal values of the acceptance threshold $w$ are easily calculated by employing numerical techniques.

## 5 Results and Discussion

The results are presented in two stages. Firstly we shall present the optimal acceptance threshold calculation for different acceptance and rejection costs rates, this is for different values of the constant $k$. Secondly, we shall show the variation of FRR and FAR in each cost case.

Exploratory analysis of the data shows that the screening variable $X$ is continuous and of the type *the larger the better*, as required by the our screening set-up, with sufficient statistics given in Table 1.

**Table 1.** Sufficient statistics for genuine and impostor for the SVM and RBF classifier.

| | SVM | | | RBF | | |
|---|---|---|---|---|---|---|
| | $\overline{x}_i$ | $s_i$ | $n_i$ | $\overline{x}_i$ | $s_i$ | $n_i$ |
| $T=1$ | 4.009 | 1.735 | 400 | 0.828 | 0.340 | 400 |
| $T=0$ | 0.306 | 0.277 | 39600 | -1.696 | 0.455 | 39600 |

In order to see how the acceptance threshold $w$ changes with the different values for $c_a$ and $c_r$, we compute optimal values of $w$ corresponding to different values of the constant $k$, $0 \le k \le 1$, for the two different classifiers, SVM and RBF. The results are shown in the following graphs,

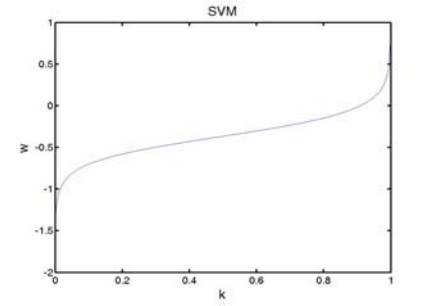


**Fig. 3.** SVM Optimal threshold

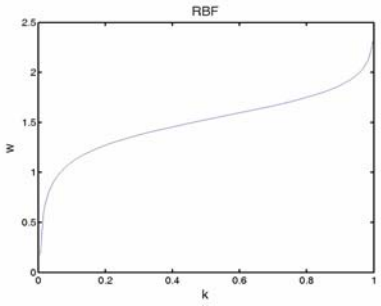


**Fig. 4.** RBF Optimal threshold

Recall that $k = c_a/(c_a + c_r)$, we now consider three specific values for the constant $k$ which may be identified with three different security levels of access control or situations, in which our face verification system may be applied.

A low security level system: In our set-up, this situation might be identify by using an acceptance cost much smaller than the rejection cost. By assuming $c_a = 0.1c_r$, for instance, we obtain $k = 0.090$. In this situation the system is will not be very restrictive and the FRR is forced to be very low. This security level could be applied in a supervised parking access control, when it is important to avoid a traffic jam.

A medium security level system is represented with equivalent rejection and acceptance cost, this is the case where we assume that a false acceptance is as dangerous (or expensive) as a false rejection. Note than then $k = 2$.

A high level security system: This could be represented by using an acceptance cost much more expensive, than the cost of rejection. For instance if we assume that $c_a = 10c_r$, the value of $k$ turns to be $k = 0.909$. In this case the FAR is nearly zero, for the RBF classifier, and null for the SVM classifier (even thought that FRR could be high). This system is highly restrictive and it could be applied to access control where we are interested in avoiding impostors to enter.

Table 2 shows the optimum acceptance threshold in three different cases: low, medium and high security level. Note that FAR decreases as security level (acceptance cost ) increases.

**Table 2.** Optimum Acceptance Threshold variation with FAR and FRR in each case.

| $c_a$ - $c_r$ rate | $k$ | SVM | | | RBF | | |
|---|---|---|---|---|---|---|---|
| | | $w$ | FRR(%) | FAR(%) | $w$ | FRR(%) | FAR(%) |
| $c_a = 0.1c_r$ | 0.091 | - 0.717 | 1 | 0.17 | 1.081 | 2.00 | 2.45 |
| $c_a = c_r$ | 0.500 | - 0.366 | 1 | 0.01 | 1.527 | 7.21 | 0.32 |
| $c_a = 10c_r$ | 0.909 | 0.001 | 3.50 | 0 | 1.888 | 11.72 | 0.31 |

Figure 3 shows the FRR and FAR for a wide variation of optimal acceptance thresholds. These results are presented in a conventional DET curve [13], which plots on a log-deviate scale the False Rejection Rate (FRR) as a function of the False Acceptance Rate (FAR). We present a DET curve of each classifier: SVM and RBF. The point of the DET curve corresponding to FNR = FPR is called Equal Error Rate (EER). While EER may not be useful in real world applications, it could be helpful in comparing the performance of systems or algorithms.

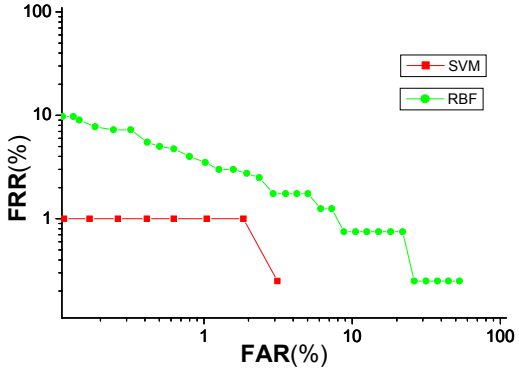


**Fig. 5.** DET curve

In this figure we can see how the SVM classifier is more reliable than RBF. If we consider the EER as a measure of the system performance the superiority of SVM is clear: EER(SVM)=0.99 and EER(RBF)=2.43.

## 6 Conclusion

In this paper we have presented a reliable face verification system with an innovate module; automatic evaluation of the optimal acceptance threshold using Bayesian screening techniques. This assure that the security level is under control while keeping a minimum error levels.

Using the algorithm proposed, the user is allow to provide the cost that is assumed to pay for false acceptance or false rejection. This allows the tailoring of our system to user security requirements. Furthermore, the user may indicate the value of the level of security required in an intuitive way, and parameter computation is hidden to

the user. The system proposed can work under several security conditions that can be changed by the user.

The method proposed is valid for all face verification systems, independently of the classifier. Its integration in an existing system has been performed and results show that integration of the algorithm is not expensive.

It is of interest to note that a face verification system may be adapted to the environment and the specific conditions of the future application in order to obtain satisfactory results.

## Acknowledgements

This paper has been supported by grants from Rey Juan Carlos University (PPR-2003-41, GCO-2003-15) and Comunidad de Madrid. The authors would like to thank Javier Arjona for his work.

## References

1. M. Turk, A. Pentland. Eigenfaces for Recognition. Journal of Cognitive Neuroscience. V 3, N 1, P 71-86. 1991.
2. P. N. Belhumeur, J. P. Hespanha, D. J. Kriegman. Eigenfaces vs Fisherfaces: Recognition using class specific linear projection. IEEE Transactions in Pattern Analysis and Machine Intelligence, Vol 19. N 7 P 711-720. July 1997.
3. L. Wiskott, J-M Fellous, N. Krüger, C. von der Malsburg. Face Recognition by Elastic Bunch Graph Matching. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol 19, Nº 7. p 775-789. Jul. 1997.
4. P. S. Penev, J. J. Atick. Local feature analysis: a general statistical theory for object representation. Network: Computation in Neural Systems. V 7, N 3, P 477-500, 1996.
5. J. J. Atick, P. A. Griffin, A. N. Redlich. Statistical approach to shape from shading: reconstruction of 3D face surfaces from single 2D images. Neural Computation. V 8. N 6. P 1321-1340. Aug. 1996.
6. R. L. Hsu. Face detection and modelling for recognition. PhD. Thesis. Michigan State University. Dpt. Computer Science and Engineering. 2002.
7. P. S. Penev, L. Sirovich. The global dimensionality of face space. Proc. Fourth IEEE International Conference on Face and Gesture Recognition. P 264-270. 2000
8. Phillips, P. J., H. Moon, S. Rizvi, and P. Rauss. 2000. "The FERET Evaluation methodology for face-recognition algorithms," IEEE Trans. Pattern Analysis and Machine Intelligence, Vol. 22, No. 10.
9. Phillips, P. J., H. Wechsler, J. Huang, and P. Rauss. 1998. "The FERET database and evaluation procedure for face-recognition algorithms," Image and Vision Computing, Vol. 16, No. 5, pp. 295-306.
10. Phillips, P. J., A. Martin, C. L. Wilson, and M. Przybocki. 2000. "An introduction to evaluating biometric systems," Computer, Vol. 33, pp. 56-63.
11. P.J. Phillips, P. Grother, R.J Micheals, D.M. Blackburn, E Tabassi, and J.M. Bone. FRVT 2002: Evaluation Report. March 2003. http://www.frvt.com
12. R. Montes Diez. Optimal Design of Two-Stage Screens: A Bayesian Approach. PhD. Thesis. University of Nottingham. Maths and Science Dpt. 2000.
13. A.Martin et al. The DET curve in assessment of detection task performance. Eurospeech 97, volume 4, pages 1895-1898, 1997.