Face Authentication For Banking

Baptiste Hemery, Julien Mahier, Marc Pasquet, Christophe Rosenberger

To cite this version:

Baptiste Hemery, Julien Mahier, Marc Pasquet, Christophe Rosenberger. Face Authentication For Banking. First International Conference on Advances in Computer-Human Interaction (ACHI), Feb 2008, Sainte luce, France. pp.137-142. hal-00255972

HAL Id: hal-00255972
https://hal.science/hal-00255972

Submitted on 14 Feb 2008

Face Authentication For Banking

B. Hemery, J. Mahier, M. Pasquet, C. Rosenberger

***Abstract*—This paper analyzes the benefit and the limitations of using a particular biometric technology "namely face authentication" for banking applications. We present first the general concepts of banking. We propose a method in order to replace the PIN code authentication by using biometrics data. Biometric authentication is then detailed. A face recognition method we developed is presented revealing as itself as a biometric candidate solution. We show the benefit and limits of this approach to be used in a real industrial context.**

***Index Terms*— banking , security, biometrics, commerce, face recognition.**

I. INTRODUCTION

Many works have been done in the scientific literature in the field of biometric authentication [16, 18]. Most of time, it concerns the definition an algorithm mainly based on image processing and pattern recognition techniques. To be used in a real context for transactions, many problems have to be solved such as the security or material aspects. Some solutions have been proposed using smart cards for example [17].

In this paper, we propose to analyze the use of a biometric information for financial transactions. Biometrics is used in the authentication process. The objective is to facilitate it and to limit banking frauds.

This paper is organized as follows. In section two, we detail the general scheme of the transaction process. We illustrate the authentication methods we can use within this context. Section three presents the general concepts of biometric authentication. A face recognition method we developed for authentication is then detailed. Experimental results of this method are given. We conclude and give some perspectives of this work in section four.

II. BANK ING

A. General architecture

The general architecture, in electronic payment, involves five partners:

- A Cardholder with his card provided by the Bank issuer,
- The bank which has issued the card,
- The Merchant who accepts the transaction with a POS[1] (or the ATM[2] in case of a withdrawal of funds),
- The Bank which acquires the transaction from the merchant or the ATM,
- The Card Scheme (Visa, MasterCard…) which has two main functions (see Figure 1):
    - A network used to transfer the authorization between the Bank issuer to the Bank acquirer;
    - An inter-banking operator which is in charge of the clearing and the settlement of the transaction between the two Banks.

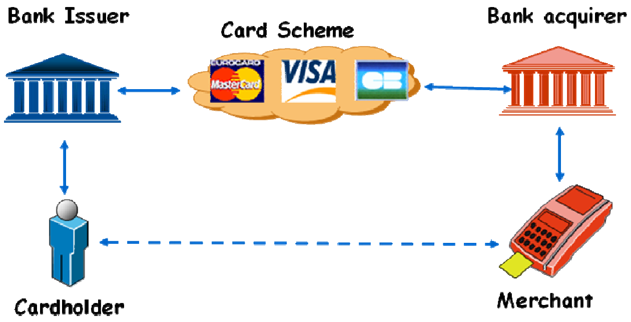


Figure 1: Relationships between the different partners

We can already identify two major transaction categories:

- Transactions initialized by smart cards: The PIN[3] code is verified by the card;
- Transactions initialized by strip cards: The PIN code is verified by the issuer.

In order to simplify the subject, in the following, we will only take the case of the smart card.

This chain implies:

- Smart Cards;
- Terminals used as a point of interaction, dedicated to operate services;
- The use of communicating devices and distant computer systems exchanging secure information via heterogeneous communication and transport networks;
- Computers and associated software required for treating, in real time the authorization and the transaction (Front End). Those devices are so outfitted with software to enable the confidentiality and the integrity of transferred data. The Front End is directly connected to a Hardware Security Modules (HSM), material and software security

B. Hemery is with the Laboratory of Vision and Robotics (LVR), ENSI de Bourges – Université d'Orléans, 88 boulevard Lahitolle, 18020 Bourges - France (e-mail: baptiste.hemery@ensi-bourges.fr).

J. Mahier, M. Pasquet and C. Rosenberger are in the GREYC laboratory, ENSICAEN - Université de Caen - CNRS, 6 boulevard Maréchal Juin - 14000 Caen - France (e-mail: Julien.Mahier@ensicaen.fr, Marc.Pasquet@ensicaen.fr, Christophe.Rosenberger@greyc.ensicaen.fr).

---

[1] POS : Point Of Sale

[2] ATM : Automated Teller Machine

[3] PIN : Personal Identification Number

devices, covering the identification – authentication of connected user.

In addition to all that devices directly implied in real time exchanges, electronic payment chain requires hardware devices and software developments (Back End) in order to allow:

- The traceability of exchanges as well as the archiving of proof, hence guaranteeing security,
- The clearing and the settlement of that financial transaction,
- The contracts management (card holder and merchant),
- The card issuing management process,
- The financial treatment of the transaction needed before sending it to the Bank Information System.

The electronic payment chain is completed (see Figure 2) by:

- A card personalization chain which allows a virgin card to be personalized for a card holder and the bank;
- A part of the Bank Information System.

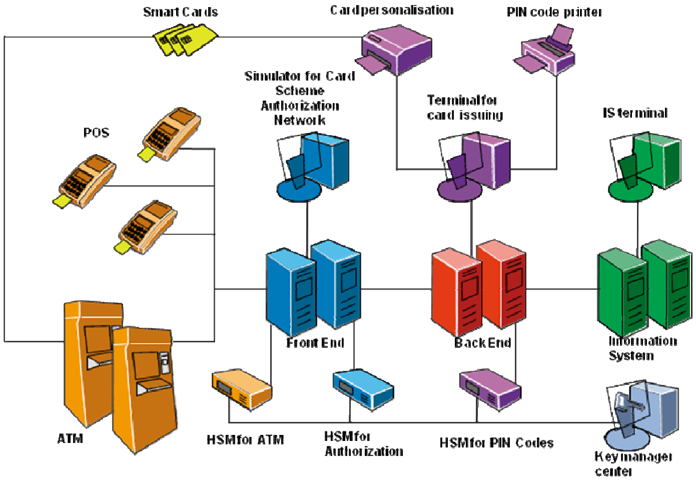


Figure 2: Electronic payment supply chain

Secure electronic transactions aim at securing and guaranteeing transactions between connected users (the cardholder and his bank issuer) for the execution of the financial service whilst integrating, over and above these purely technical aspects, user acceptance implying reinforced confidence and greater value in use. It is the reason why the problem of the cardholder authentication is so important for the financial services

B. *Authentication by PIN code*

One individual has three possibilities to prove its identity:

- What he owns (card, document) ;
- What he knows (a name, a password) ;
- What he is (fingerprint, hand, face...)

Actually, bank payment chain uses mainly the first two types of proof:

- Card to identify the cardholder and so to authenticate the card with the use of cryptographic keys and certificates,
- Password to authenticate the cardholder.

It should be very interesting to use, in place of the PIN code which represents only four figures to guess, but that we have difficulties to memorise when we have few different cards with few different codes, a biometric authentication very difficult to guess and that you wear with you wherever you go.

For this particular case of the electronic payment with a smart card, the biometric reference information is stored in the card. The card calculates a matching measure between the information stored on it and the information transmitted by the POS. However, the biometric analysis and the treatment to obtain a digital signature will be realized by the POS itself. It will compare a variable signature (slightly different of the enrolled signature) and require large calculation possibilities that can be at the limits of the actual low-cost cards. So, a particular attention must be brought on this point in the future implementation.

C. *Biometric authentications: existing solutions*

In term of electronic payments, banks have tested four main biometric solutions:

- Fingerprint; a solution is already operational on certain POS (Sagem…) (see Figure 3).

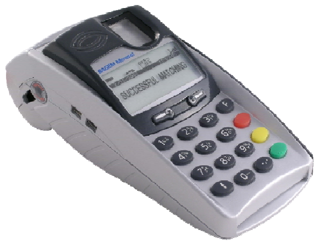
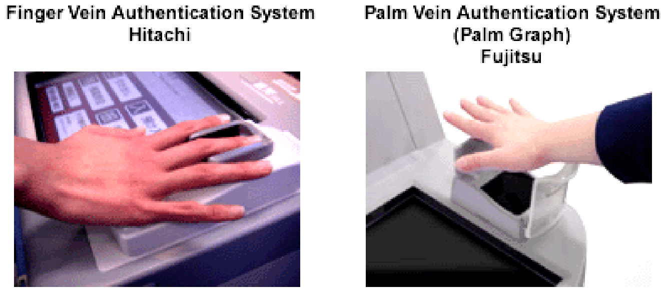


Figure 3: Biometric POS with fingerprint sensor

- Finger and palm vein authentication; useful solution for ATM but not on POS due to the sensor cost (Figure 4).


Finger Vein Authentication System
Hitachi
Palm Vein Authentication System
(Palm Graph)
Fujitsu

Source: Hitachi, Fujitsu

Figure 4: Different biometric solutions used actually in Japan.

- Iris; useful solution for ATM (normalized trough Iriscode®) but not on POS due to the sensor cost (see Figure 5).

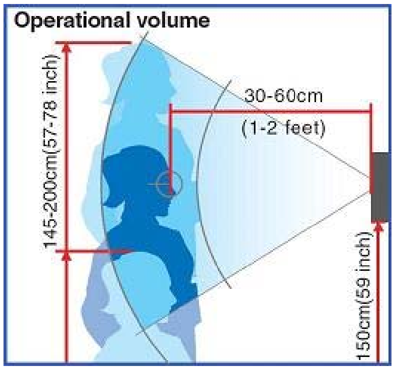


Figure 5: A biometric solution based on the iris information.

These existing solutions use some biometric modalities. In the following section, we present a state of the art in biometric modalities use for different applications.

III. BIOMETRICS

Biometrics technologies are present in our daily life, for instance: passport, access control and even when we are walking in the street.

A. General principle

Biometrics embed different physiological or behavioral characteristics of an individual. These data are useful to identify or authenticate an individual for different applications (crime, access control…).

The goal of biometrics is to answer two questions:

- « Who am I ? » It concerns the identification of an individual among N possible ones (1 against N) ;
- « I Am M. X ? ». It is the authentication that seeks to guarantee the identity of an individual (1 against 1).

B. Biometric modalities

There are currently many biometrics data for the authentication of an individual:

- biological analysis: odor, blood, saliva, urine, ADN…
- behavioral analysis: online signature, keystroke, voice,…
- morphological analysis: fingerprints, hand geometry, features of the face, drawing of the venous network of the eye,….

Biometric authentication for banking customers are much more currently advanced in morphological analysis for several reasons:

- the sensors are currently more reliable, more efficient than the biological analysis and cheaper;
- pattern recognition algorithms used in morphological analysis are well known, even if some Japanese banks actively worked on online recognition of the signature [15];
- recognition times for the morphological information are often shorter than for the two other types of analysis;
- user perception of the intrusion of these technologies in its sphere of protection (perceived technologies as more or less invasive) is often better for certain morphological analysis.

The morphological analysis can be carried out starting from various parts of the human body (see Figure 6). Some analysis are rather well tested, others are more innovative:

Figure 6: Different biometrics modalities (DNA, hand geometry, fingerprint, iris)

- Fingerprints acquired by optical sensors, with silicon (piezoelectric effect, capacitive, thermoelectric and photo electric) ultrasonic, electromagnetic [12-13]: This is most well known technique. The use of the fingerprints for the identification of an individual is not new. In fact, police forces have used this technique for more than 100 years by analyzing particular points called "minutiaes". In order to carry out this analysis, between 10 and 100 minutiaes are necessary. The use of fingerprints counts for more of 60% of the market of the biometric processes (see Figure 7, AFIS/ Line-scan is also based on fingerprints). Fingerprints are generally easier accepted by the community and that it is one of most effective and of the less expensive.

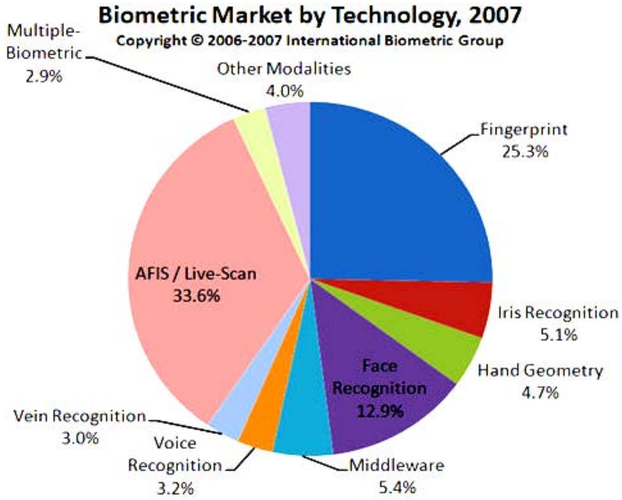


Figure 7: Biometric market and repartition of the different modalities

- The hand geometry analysis is a popular technology which is largely employed for the physical access control or the time pointing. It is very simple and cheap. The performance of a biometric system based on the hand geometry is completely reasonable. The elements taken into account rest only on the geometry of the hand and not on the palmar print. The system takes a picture of the hand and examines 90 characteristics, including the three-dimensional shape of the hand: the length and the width of the fingers, the shape of the articulations.

- The position of the veins of the hand: It is a very promising technology and not a very invasive implementation by a large Japanese bank on more than thousand agencies [16]. An infrared camera takes a picture of the hand under two different angles to obtain an information in three dimensions. The definition of the several interception of the veins of the hand with a sphere of reference makes it possible to work with less than 10 characteristic points.
- The face analysis is based on several pattern recognition techniques, but for the majority it is of interest which these techniques base on elements of the face which are the least suitable for changes [3,9]: large higher features of the orbits, sectors surrounding the knobs, sides of the mouth and other characteristics similar in order to be robust face to the changes as haircut.
- Iris of the eye: After the digitalization of the image of the eye by a camera, the software determines the center of the pupil and the zone where the iris is. Then, on two angular sectors, the software cuts out bands of regular size there and generates a gauge from the local analysis of the texture of the iris [14]. This fast and reliable technology is already used in certain banking experiments.
- Veins of the retina. After the capture of an image of the retina, the software of the reading device cuts out a ring around the fovea. In this ring, it locates the site of the veins and their orientation. Then, it codifies them in a gauge. The operation in itself is rather simple but is perceived like relatively invasive by the worn ones.

C. Face recognition

Among all biometrics techniques, face recognition is a great challenge. First, face recognition is a contact less technique, this is important for hygienic aspects. Second, it uses a cheap sensor namely a CCD that could be easily embedded in a cash distributor. Last, this authentication process is not very constraining for an user. Nevertheless, many problems can occur like illumination changes or face orientation variations during acquisition. Moreover, many aspects of an individual can change with time (haircut, glasses wearing, etc.).

A lot of research has been done in the field of face recognition in order to improve the robustness of algorithm face to these variations [3,9]. Classical approaches are based on data reduction with different methods like PCA [10] or more sophisticated ones like Fisherface [11]. We propose in this paper a new face recognition method based on previous works we realized in 2006 [19].

D. Developed method

The originality of the proposed algorithm is the use of invariant descriptors for the characterization of the face of an individual. Un invariant descriptor has the property to have a similar value for different viewpoints. This is for us an important property for a face recognition method. We defined two approaches. In the local approach, invariant descriptors are computed in the neighborhood of extracted keypoints on the face of an individual. In the global approach, they are calculated on the whole image. The general scheme of the proposed method is illustrated in Figure 8.

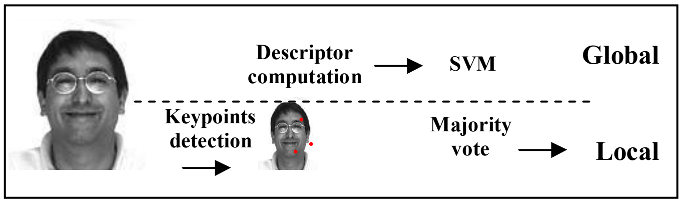


Figure 8: General scheme of the proposed method

1) Zernike moments

In 1934, Zernike introduced a set of complex polynomials which forms a complete orthogonal set over the interior of the unit circle, i.e., $x^2 + y^2 \le 1$. Let $\{V_{nm}(x,y)\}$ be the set of polynomials. The form of these polynomials is :

$$\begin{gathered} ZP = \left\{ V_{nm}(x,y) \middle| x^2 + y^2 \le 1 \right\} \\ V_{nm}(x,y) = V(\rho,\theta) = R_{nm}(\rho)\exp(jm\theta) \end{gathered} \tag{1}$$

Where:

n is a positive integer or zero.

m is a positive and negative integer subject to constraints $n-|m|$ even, $|m| \le n$.

ρ is the length of vector from origin to (x, y) pixel.

θ Angle between vector ρ and x axis in counter clockwise direction.

$R_{nm}(\rho)$ Radial polynomial defined as:

$$R_{nm}(x,y) = \sum_{s=0}^{(n-|m|)/2} (-1)^s \frac{(n-s)!}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n+|m|}{2}-s\right)!} \left(x^2+y^2\right)^{(n-2s)/2} \tag{2}$$

Note that $R_{n,-m}(\rho) = R_{n,m}(\rho)$.

Zernike moments are the projection of the image function on these orthogonal basis. The expression of Zernike moments of order n with repetition m is given below:

$$A_{nm} = \frac{n+1}{\pi} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x,y) \left[V_{nm}(x,y) \right]^{*\;4} \tag{3}$$

To compute the Zernike moments of a given image, the center of the image is taken as the origin and pixel coordinates are mapped to the range of unit circle, i.e., $x^2 + y^2 \le 1$. The pixels falling outside the unit circle are not used in the computation. Also note $A_{nm}^{*} = A_{n,-m}$.

---

[4] * denotes conjugate complex number

Zernike moments are well known to be rotation invariant. In order to obtain the translation and scale invariances, a shape is normalized by obtaining the smallest circle centered at the center of mass, covering all the shape pixels [8]. The obtained circle is then adjusted to match the radius of Zernike moment basis functions.

2) *Keypoints detection*

The use of local points to describe the face is very interesting because it makes possible the recognition of an individual even if some parts are not similar. As for example, Figure 9 shows the keypoints detection results (with the Harris detector) for the same individual. We notice that some points are present at the same location for the two images (mouth for example).

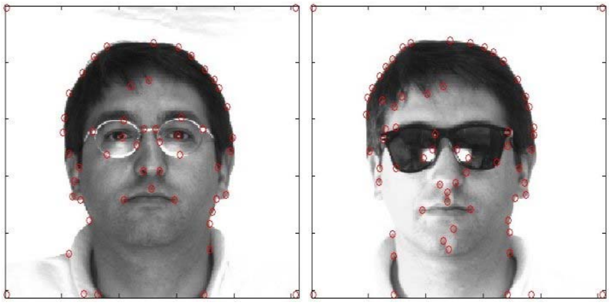


Figure 9: Keypoints detection results for two images of the same individual.

Lots of keypoints detectors have been proposed in the literature [7]. They are either based on a preliminary contour detection or directly computed on gray-level images. The Harris detector [6], that is used in this article, belongs to the second category. It is consequently not dependant of a prior success of the contour extraction step. This detector is based on statistics of the image and rests on the detection of average changes of the auto-correlation function. The average number of detected keypoints is around 50 for the used images. Figure 10 presents the interest points and the associated neighborhood obtained for one individual extracted from the AR face database [3,4]. Local descriptors are then computed on the neighborhood of interest points.

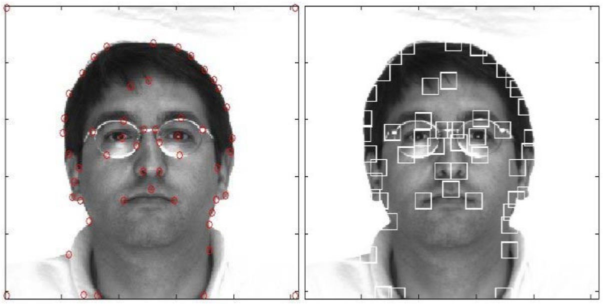


Figure 10: Keypoints detection and associated neighborhood for the same individual

3) *Learning and recognition*

Once an individual is described by the previous moments (computed on multiple locations for the local approach), we use a supervised classification method with a learning database for the recognition step. In this section, we describe the classification block based on support vector machines (SVM).

SVM were proposed by Vapnik [1]. This method creates functions from set of labeled training data [2]. The function can be a classification function with binary outputs or it can be a general regression function. For classification, SVMs operate by finding a hypersurface in the space of possible inputs. This hypersurface attempts to split the positive examples from the negative examples. The split will be chosen to have the largest distance from the hypersurface to the nearest of the positive and negative examples. Intuitively, this makes the classification correct for testing data that are near, but not identical to the training data. We can use a one-class SVM for an authentication problem or multiple classes SVM for an identification one.

In the local approach, the decision result takes into account the recognition result for each keypoint. The majority vote procedure is then applied to determine the authentication/identification result of an individual

E. *Experimental results*

In order to test the proposed approaches, we used the AR face database [4,5]. This database contains frontal images of 120 individuals, 65 males and 55 females. Images were realized in two different sessions two weeks apart. During each session, 13 pictures were taken with different facial expressions (see Figure 11), illumination variations (see Figure 12) and occlusions (see Figure 13).

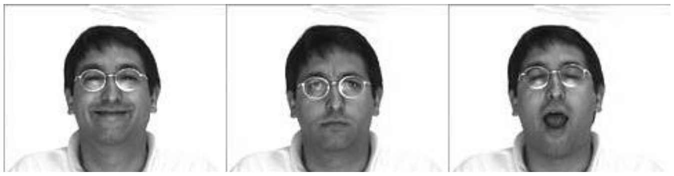


Figure 11: Samples of face with different expressions.

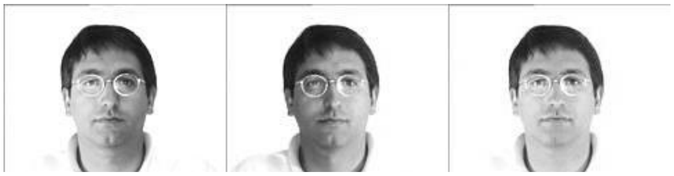


Figure 12: Samples of face with different illuminations.

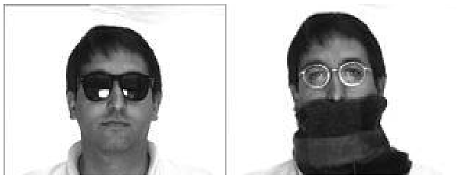


Figure 13: Samples of face with different occlusions

A first experiment was realized with 50 individuals randomly chosen and with only non-occluded images (without sunglass nor scarf). The training set was created by using randomly chosen images of these individuals. This process was repeated ten times and the average results are shown in Table 1. For example, if there are 5 images per individual in the training set, the test set is constituted of the 9 others of these individuals. The best results are obtained by the DCV method [20]. The proposed method denoted LZMV (Local Zenike Majority Vote) after optimization of its parameters (denoted LZMV*) provides a result not very far from DCV.

Method	Recognition result
GZ	96.68%
LZMV	97.48%
LZMV*	**98.63%**
Fisherface [11]	98.85%
EigenFace [20]	79.14%
DCV[20]	**99.65%**

Table 1: Recognition results (GZ : Global Zernike, LZMV: Local Zernike Majority Vote, LZMV*: optimized version of LZMV)

We then made a second experiment to evaluate the robustness of the proposed algorithm. Such studies have not been done by others algorithms in the state of the art. In this experiment, pictures of 120 individuals were used. The training set is composed with only the two pictures per individual without any perturbation. We then tried to recognize images with expression, illumination and occlusion alterations. Results of this experiment can be seen in Table 2.

Method	a	b	c
Global	**92.63%**	**81.52%**	**44.37%**
Local	87.63%	41.38%	37.15%

Table 2: Recognition rate for each approach and different perturbations: (a: Expression, b: Illumination, c: Occlusion)

The robustness of the global approach is much better than the local one. Occlusion seems to be the most important challenge for the authentication process. Nevertheless, an individual who wants to be authenticated has no reason to hide one part of its face.

IV. CONCLUSION

In this paper, we studied he benefit and limitations of using biometric technologies for bank payment. Biometric has the goal to avoid some frauds and to facilitate the authentication process for an user.

Biometrics has many problems to solve before been used in a real industrial context for banking applications. The performance of biometric algorithms provide globally good results. But, if we consider the face recognition method we presented in this paper, if the face of an individual is occluded, we may have some authentication errors. Many problems have also to be solved in order to use biometric data in the existing banking architecture while preserving the security of transactions. We attend to work on these aspects in the future.

REFERENCES

[1] V. Vapnik, “Suppport-Vector Network”, Machine Learning, vol. 20, issue 3, September 1995, pp. 273-397.

[2] J. Platt, “Support Vector Machines”, http://research.microsoft.com/users/jplatt/svm.html, 2003.

[3] Yuxiao Hu, Dalong Jiang, Shuicheng Yan, Lei Zhang, Hongjiang Zhang, Automatic 3D Reconstruction for Face Recognition, in Proc. *6th IEEE International Conference on Automatic Face and Gesture Recognition (FG)*, Seoul, Korea, 2004

[4] A.M. Martinez and R. Benavente, http://rvl1.ecn.purdue.edu/~aleix/aleix/face/DB.html

[5] A.M. Martinez and R. Benavente, “The AR face database”, CVC Tech. Report, vol. 24, 1998

[6] C. Harris and M. Stephens, “A combined corner and edge detector”, Alvey Vision Conference, pp. 147-151, 1988

[7] C. Schmid, R. Mohr and C. Bauckhage, “Evaluation of interest point detectors”, International Journal of Computer Vision, vol. 37, pp. 151-172, (2), 2000

[8] S. M. Abdallah, E.M. Nebot, et D.C. Rye “ Object Recognition and Orientation via Zernike moments”. In Chin, and Pong, T .C. editors, Proc. Computer Vision ACCV’98, volume 1 of LNCS 1351, pages 386-393. Springer Verlag, 1998.

[9] Xiaoming Liu and Tsuhan Chen , “Pose-Robust Face Recognition Using Geometry Assisted Probabilistic Modeling” Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), vol. 1, pp. 502-509, 2005

[10] Matteh A. Turk and Alex P Pentland, “Face Recognition Using Eigenfaces”, Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), pp. 586-591, 1991

[11] Peter N. Belhumeur, Joao P. Hespanha and David J. Kriegman, “Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection”, IEEE Transactions on pattern analysis and machine intelligence, vol. 19, pp. 711-720, (7), 1997

[12] S. Cruz-Llanas D. Simon-Zorita, J. Ortega-Garcia and J. Gonzalez-Rodriguez, “Minutiae extraction scheme for fingerprint recognition systems”, 2001.

[13] V. Espinosa, “Minutiae detection algorithm for fingerprint recognition”, IEEE AESS Systems Magazine, pages 7–10, March 2002.

[14] Yunhong Wang Li Ma, Tieniu Tan and Dexin Zhang, “Personal identification based on iris texture analysis”. IEEE Transaactions on Pattern Analysis and Machine Intelligence (25) December 2003.

[15] I. Yoshiaki, S. Yoichi, K. Naohisa, “Proposal of Biometric Authentication Model Using Digital Signature Technologies and Development of its Prototype System”, Journal of the Institute of Image Electronics Engineers of Japan, vol. 33, pp. 161-170, 2004

[16] M. Watanabe, T. Endoh, M. Shiohara, and S. Sasaki “Palm vein authentication technology and its applications”, Proceedings of the biometric consortium conference, 2005.

[17] Y. Chemla and C. Richard, “A security device, method and system for financial transactions, based on the identification of an individual using a biometric profile and a smart card”, patent n° PCT/FR2006/000382, 2006.

[18] R.R. Vangala and S. Sasi, “Biometric authentication for e-commerce transaction”, IEEE International Workshop on Imaging Systems and Techniques, pp. 113- 116, 2004.

[19] B. Hemery, C. Rosenberger, C. Toinard, B. Emile, "Comparative study of invariant descriptors for face recognition", 8th International IEEE Conference on Signal Processing (ICSP), vol. 2, pages 16-20, 2006.

[20] Mitch Wilkes Hakan Cevikalp, Marian Neamtu and Atalay Barkana. Discriminative common vectors for face recognition. IEEE Transactions on pattern analysis and machine intelligence, 27(1) pages 4–13, January 2005.