# Moving Face Spoofing Detection via 3D Projective Invariants

Maria De Marsico
Sapienza Università di Roma
v. Salaria 113, 00198, Rome (IT)
demarsico@di.uniroma1.it

Michele Nappi
Università di Salerno
v. Ponte don Melillo, 84084, Fisciano (IT)
mnappi@unisa.it

Daniel Riccio
Università di Salerno
v. Ponte don Melillo, 84084, Fisciano (IT)
driccio@unisa.it

Jean-Luc Dugelay
Institut EURECOM,
Sophia Antipolis, (France)
dugelay@eurecom.fr

## Abstract

*Face recognition provides many advantages compared with other available biometrics, but it is particularly subject to spoofing. The most accurate methods in literature addressing this problem, rely on the estimation of the three-dimensionality of faces, which heavily increase the whole cost of the system. This paper proposes an effective and efficient solution to problem of face spoofing. Starting from a set of automatically located facial points, we exploit geometric invariants for detecting replay attacks. The presented results demonstrate the effectiveness and efficiency of the proposed indices.*

## 1. Introduction

Most commercial face recognition systems operate on 2D images, in visible or infrared light. Their sensitiveness to spoofing can significantly vary [12]. Poor or absent spoofing detection implies that a system can be cheated by simply showing a photo of a registered user. Detecting the movement of the face or of some parts (smile, eye blinking) [13] can avoid this; however, even these countermeasures can be cheated by a video clip of a registered user. To address this, more elaborate anti-spoofing techniques aim at verifying the actual three-dimensionality of the face in front of the capturing device. Though in a complicated way, even such systems can be cheated through 3D models of the face [12]. Finally, 3D verification can be cheated by a 3D mask, with overlaid realistic face texture, which is quite difficult, time-consuming and expensive to make [16], as well as by *photographic masks* [7], i.e. high resolution photographs of a face, where the eyes and the mouth were cut out, with the impostor looking through like in a mask. Few works address the mask problem.

It appears that a robust anti-spoofing technique must rely not only on verifying captured face three-dimensionality, but also on a specific user interaction with the system. This follows a challenge-response protocol, similar to those attempting to prevent malicious automated software from performing massive sets of actions to degrade the quality of service of a system. The system requires a specific action ("challenge") from the user. In the case of face recognition this is the request for face changes, such as smiling or eye blinking, or the pronunciation of a specific sentence; then, the system analyses the change and checks that the user actually carries it out ("response"). Since the gesture/expression to detect is system-triggered, of well-determined kind, and occurs in a specific time elapse, the associated recognition procedure can be considered quite affordable, though requiring additional equipment/software. In order to avoid spoofing through a pre-recorded video, challenge may even be simply based on the time of requested motion, instead of also demanding for a specific motion type. We will return on this in the following. Extra-hardware might support the recognition system, by further detecting user's image liveness (e.g. through a thermal sensor). However, this kind of countermeasure increases the cost of the system, yet without assuring the optimal performance (in the same example, a thermal sensor without any further measure might be deceived by a fake fingerprint on a "live" finger, or a mask on a real face). The presented method has the advantage to exploit face 3D information, though at a much lower computational cost than traditional techniques. At the same time, it does not require the user to stay always in a perfect frontal pose and looking towards the capture device, as it is often the case in eyeblink-based techniques. As a matter of fact, our method provides a sufficient tolerance to user's position, given that face rotation is not excessive (e.g., profile pose). Experimental results show that the spoofing detection algorithm we propose is able to detect spoofing attacks to the system both quickly and with high accuracy.

## 2. Related work

In 1999, Choudhury *et al.* presented one of the first approaches to liveness detection based on the estimation of the 3D structure of the face [3]. Its main limit is its sensitivity to image quality. The latter is a crucial requirement also for those techniques that are based on the analysis of non-rigid local deformations of facial components, which are further sensitive to bending and to motion depth of a photo. Among these, [6] is based on optical flow. Input quality is a sore point also for the technique proposed by Li *et al.* [9]. This is based on the



978-1-4673-0397-2/12/$31.00 ©2012 IEEE

observation that the Fourier spectrum generated by a photo presents significant differences with that by a live face. It is possible to improve the anti-spoofing performances by substantially increasing the interactive collaboration required from the user and by fusing more modalities, like in Frischholz and Dieckmann [5] who fuse face and voice. Of course, the system computational resources need to be increased too. Along the line of exploiting users' interaction, the main goal of the present work is to define a technique assuring the same accuracy of a 3D system, yet with a much more limited amount of resources. Moreover, it is uniquely based on measures from a set of easy-to-detect facial points. Therefore, it can also process low quality inputs. Though the user is randomly requested to move the head, it is not necessary to perform a specific motion, so that also the amount of necessary user thoroughness is somehow limited. Therefore, the presented technique is perfectly consistent with the requirements identified by Pan *et al.* in [13]. Of course, the problem of implementing an effective as well as efficient technique to verify the true three-dimensionality of the face during the capturing phase is harder to address. Projective invariants are a valid solution.

The main difficulty in recognizing objects from images is that their aspect depends on the point of view. One method to overcome this issue is using a descriptive geometry, which is not influenced by object transformations. Many studies in literature deal with 3D object descriptors, which are invariant to projective transforms [2]. They are very important for all those approaches that aim to 3D object recognition starting from 2D images. However, Burns *et al*. [2] demonstrated that any descriptor which is invariant to a group of transforms (affine, projective, rigid) must necessarily comply with some constraints (point collinearity, point coplanarity, as well as the contrary, etc.). In fact, many descriptors rely on the distance ratio among collinear or coplanar points. In [14], geometric invariants have been applied to the face by defining an asymmetric protocol 3D/2D: enrolment is performed in 3D while identification is performed from 2D images, to have more robust face recognition while keeping the system practical. In this work, the same mathematical definition of geometric invariants is exploited, but these are used according to reverse considerations. Given a configuration of points on an object, which are known as not coplanar, a geometric invariant which would instead require coplanarity is computed from them, on more consecutive images. If the invariant is respected, points must be coplanar; this would not be possible assuming a 3D face, and therefore the object is not 3D. By applying this argument to face recognition, we can distinguish a real face in front of a capture device from a picture.

## 3. Face location and preprocessing

A face detection module analyzes each input frame and returns the detected face. Location is performed by implementing a cascade combination of the Viola-Jones' algorithm with an Extended Active Shape Model, realized by STASM software as in [11]. STASM searches relevant landmarks by minimizing a global distance between candidate image points and their homologues on a general model (shape model), which is pre-computed over a wide set of training images. 68 interest points are located, a subset of which is used for invariants computation. The precise distribution of such points is available in [10]. Though STASM is sensitive to poses far from frontal, recent techniques significantly improve precision [1].

## 4. Projective Invariants

For readers' convenience, we report here the mathematical definition of the exploited invariants [14]. Given *inhomogeneous* coordinates $x=(x^1, x^2, \ldots, x^m)^t$, where $x \in R^m$, the corresponding *homogeneous* coordinates of the point are $z=(z^1, z^2, \ldots, z^{m+1})^t$, where $x^l=z^l / z^{m+1}$, $l=1,2,\ldots,m$ and $z^{m+1} \neq 0$. The homogeneous coordinates are a more general representation of points, requiring that $\exists\, l \in \{1, 2, \ldots, (m+1)\} \ni z^l \neq 0$. Through this mapping, the projective transformation in $R^m$, can be easily managed as a linear transformation in $R^{m+1}$. If we represent the new points coordinates in matrix form, most ratios among distances in space can be represented as ratios of determinants (see also (1) and (3) below) of the corresponding matrices. We will use homogeneous coordinates from this point on. We now consider invariants, which can be divided in two main categories. The first category, namely 2D based invariants, does not require computation of the 3D object model. However, constraints about the localization of feature points (collinearity or coplanarity) are quite stringent. On the contrary, the second category, namely 3D image based invariants, requires a 3D object or at least 3 different points of view of it. On the other hand, it is very flexible about the repartition of the anchor points. In this work, only 2D image based invariants are considered. Given four collinear points $z_1, z_2, z_3, z_4 \in R^2$, the simplest invariant is their cross ratio, that can be written as:

$$cl = \frac{M(1,3) \cdot M(2,4)}{M(1,4) \cdot M(2,3)}, \text{ with } M(i,j) = \begin{vmatrix} x_i & x_j \\ 1 & 1 \end{vmatrix} \quad (1)$$

As shown in Fig. **1** (a) this geometric invariant can be seen as the ratio of distances (AC/BC)/(AD/BD). The cross ratio of four collinear points, also known as the *anharmonic ratio,* depends on the labelling of the points, therefore different orderings of the labels yield *24* possible cross ratios; however, only six of them have distinct values, and,

given one invariant, all the others are functionally dependent from it, i.e. can be derived from it.
A further generalization is represented by the cross ratio of five points on the same plane (Fig. **1** (b)). Five coplanar points yield two functionally independent invariants:

$$cp_1 = \frac{M(1,2,4)\cdot M(1,3,5)}{M(1,2,5)\cdot M(1,3,4)}\ ,\ cp_2 = \frac{M(2,1,4)\cdot M(2,3,5)}{M(2,1,5)\cdot M(2,3,4)} \quad (2)$$

$$\text{with } M(i,j) = \begin{vmatrix} x_i & x_j & x_k \\ y_i & y_j & y_k \\ 1 & 1 & 1 \end{vmatrix} \quad (3)$$

These invariants can be interpreted geometrically by considering all lines passing through $x_1$ and connecting it to the other points, that give a cross ratio $cp_1$ of four lines.

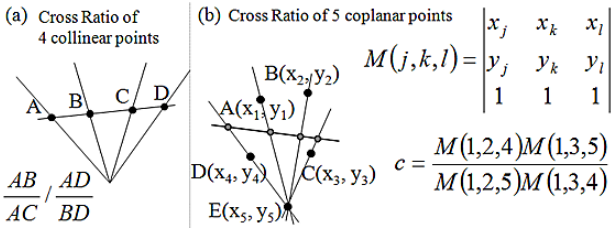


Fig. 1. Cross ratio: four collinear (a) and five coplanar points (b).

This is the dual problem of four collinear points (shown in Fig. **1** (b) as well), with respect to the *fundamental theorem of the invariant geometry*. The second invariant $cp_2$ is computed in the same way, with respect to, say, $x_2$,. It is possible to prove that all the other invariants which can be obtained with different pairs of points are functionally dependent on $cp_1$ and $cp_2$. If collinearity/coplanarity constraints are satisfied, cross ratios are rotation invariant, and can be used to devise robust recognition methods.

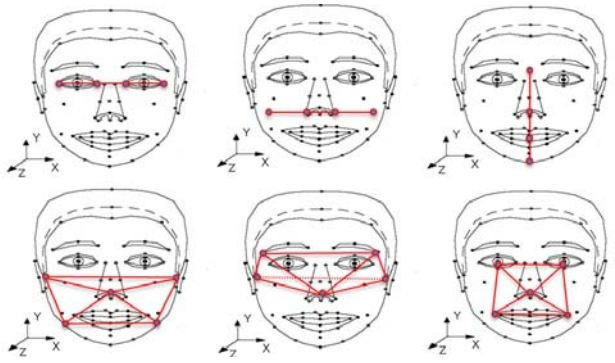

Fig. 2. Configurations of points chosen to compute cross ratios $c_1$, $c_2$, $c_3$, $c_4$, $c_5$, $c_6$ (from left to right and from top to bottom).

Projective invariants are particularly useful and easy to exploit when handling rigid solid objects. Unfortunately, that is not the case of faces, because they undergo to deformations due to expression variations. A further difficulty is the identification of points complying with collinearity or coplanarity constraints. Fig. 2 shows the configurations of points which have been considered to compute cross ratios c1, c2, c3 (first row, collinear points) c4, c5, c6 (second row, coplanar pints) which were tested for their contribution to solve our problem. With respect to the invariants exploited in [14], we selected a different subset (except for c1) because it proved to be more suited to the new problem at hand.

## 5. Detecting spoofing attacks

The most robust spoofing detection systems in the field of face recognition rely on two main activities: 1) verification of face three-dimensionality, 2) interaction with the user. The first may require implementing very sophisticated techniques, while the second, in most cases, involves additional hardware and software such as, for example, when the user is asked to pronounce a specific sentence. Interaction may be modelled according to two parameters: time and content, e.g. motion type. Requiring motion at a random time is sufficient to avoid an attack through a pre-recorded video. In particular, it is a possible countermeasure against replay-attacks: since challenge times between different accesses, and therefore the expected response times, can significantly change, it is highly improbable to be able to use previously stolen authentication credentials. However, challenge-response may be spoofed by video, if for example the system would always ask a basic and always the same head motion, e.g. turn your head from left to right. This latter attack can be successfully addressed by requiring a random yet specific motion type, but this asks for a 3D model to track such motion and distinguish it from an appropriately presented photo. This enhances spoofing defence, but at the expense of a significant increase of system complexity.

In this work we rely on a quite novel way of using projective invariants to obtain similar results, but with lower complexity, improving system efficiency. We exploit motion time, but we get rid of controlling the exact motion type, given that true three-dimensionality can be verified. Not requiring an exact pose is a significant strength of our approach. The user can move more freely, and therefore feel more comfortable. Moreover, we do not have to check the exactness of the taken pose. We rather exploit it to check three-dimensionality of the face. In conclusion, when the user is in front of the system, this requires to perform a generic and continuous face motion. The request is issued at random times. We assume to work in a setting were user is possibly cooperative, and is aware that at least a minimum amount of move is required. Otherwise, we might obtain a false reject, calling for a new testing without compromising the system security.

## 6. Cross ratios against spoofing

As explained above, cross ratios are invariant to rotations if and only if the points from which they are computed satisfy specific collinearity or coplanarity constraints. Suppose to reverse the argument. We detect the lack of three-dimensionality of an object when, once selected a set of its points which is known to be not coplanar in 3D (e.g. centre of eyes, nose tip, and chin for the face), the cross ratio computed starting from them is constant across different object positions (face poses). In other words, if the pose of the subject in front of the capture device changes, but the computed cross ratio stays constant, the points from which it is computed must be coplanar; however, since they cannot be so by definition in 3D, it must be that we are rather processing a 2D representation (a photo) of the face. To add a spoofing detection-oriented interaction, the system requires to move the face, and only in those well-defined time intervals the cross ratio will be verified.

A crucial element is represented by the choice of the cross ratio to use as a discriminative criterion. Intuitively, the best candidates for the specific goal are those points that in a real 3D face model strongly violate collinearity/coplanarity constraints, but strictly satisfy them in a possible two-dimensional representation (photo) of the same model. To this aim, we considered 3 cross ratios of four collinear points and 3 cross ratios of five coplanar points, which are shown in Fig. 2. The reason for the collinear ones is just to demonstrate that they are not useful to refute the three-dimensionality hypothesis.

The system randomly asks the user to move the face, while the capture device takes a sequence of images. Each image is processed to locate the facial points which are used to compute the cross ratios. In a 3D face, the points do not satisfy the coplanarity constraint, and therefore the cross ratios will not be stable; on the contrary, they will undergo a variation whose extent will be measured. In detail, the system implements the following algorithm:

```
for each captured frame I
   detect facial points P from I;
   compute the cross ratio c_j from P;
   compute on last k frames
          m_j=(1/k) ∑c_j          (mean)
          v_j=(1/k) ∑|c_j-m_j|    (variation)
   if v_j > th_j
      genuine = genuine + 1;
   end
end
if (genuine)/(number of processed frames) > th_v
 return "Genuine User"
else
 return "Spoofing Attack"
end
```

The variation $v_j$ of a cross ratio $c_j$ is computed over the last $K$ frames (*observation window*) and compared with a predetermined threshold $th_j$, which is generally different for each cross ratio. In addition, the number of frames rated as genuine (that is $v_j > th_j$) must be higher than a further predetermined threshold $th_v$, which is set also according to the required level of security. Frames which present location errors, i.e. no located faces, or incorrectly determined points, are discarded, so that they do not enter the *observation window*. In particular, correctness of the location of points is estimated by measuring Euclidean distances among corresponding points in pairs of successive frames. This helps dealing with location noise. Finally, the number of considered frames $K$ is a crucial parameter in terms of system performances, as will be shown in the following.

## 7. Selection of suited cross ratios

The six cross ratios for the configurations in Fig. **2** were evaluated on data collected from 10 different users, both through direct capture, and through printed images to simulate spoofing, for a total of 20 acquisitions. The aim was to determine which configurations better support discriminating genuine accesses from spoofing attacks.

In the sequences of genuine attempts, the subject is in front of the capture device and, when asked by the system, moves the face. In sequences of spoofing attempts, a photo is presented, and, when asked by the system, the impostor varies the photo orientation in front of the capture device. Each configuration for cross ratio was separately tested on the two groups of 10 acquisitions (genuine attempts, spoofing attempts). Fig. 3 shows graphs of the variability of cross ratios in one of the performed experiments, which summarizes the general trend of the behaviour of the different cross ratios on all the simulations.

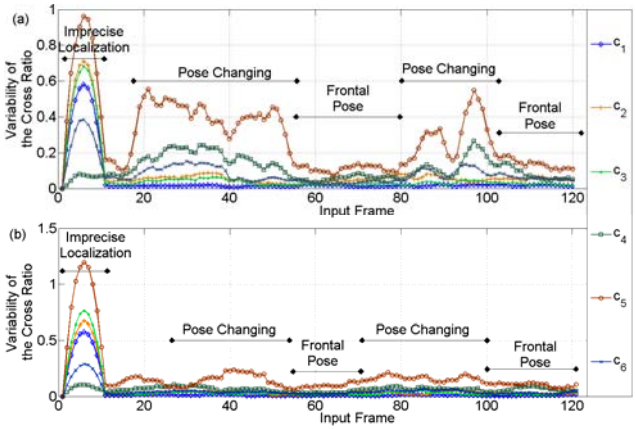


Fig. 3. Curves produced by cross ratios $c_1$, $c_2$, $c_3$, $c_4$, $c_5$, $c_6$ in one of the experiments (top: genuine access, bottom: spoofing attack)

The curves show that cross ratios computed from four collinear points, collinearity constraints are always satisfied, such that the related variation $v_i$ (i=1,2,3) is

always low, both for genuine attempts (a) and for spoofing ones (b). On the contrary, the trend of variation $v_i$ (i=4,5,6) for the cross ratios from coplanar points, undergoes a significant variation for real users (a), which is missing in spoofing attempts (b). Fig. 3 highlights a high variability of the initial part of all curves, since not all *K* frames (10 here) needed to compute $v_i$ had been processed yet. This may also happen when location is wrong, so introducing an extra variability which is not due to three-dimensionality. This limit can be overcome, by observing that these errors contemporarily affect cross ratios of collinear points. Therefore, the system can control at the same time both $v_1$ and $v_5$, and analyze only values of $v_5$ for which $v_1$ has a low value (correctly processed frame). Notice that the database used for this $c_1$-$c_6$ invariants evaluation is not that used for the following tests. The obtained good results further assessed the generalizability of the invariants selection for the problem at hand.

## 8. Assessing anti-spoofing performances

The experiments had the twofold goal of evaluating the best system parameters configuration and of measuring its accuracy performance. As for accuracy we mean the system ability to distinguish genuine subjects from "dummy" ones (photo); it was measured in terms of Equal Error Rate (EER), by considering as False Acceptance Rate (FAR) the rate of "dummy" subjects classified as genuine, and as False Rejection Rate the rate of genuine users that were rejected as "dummy". The system was tested with 20 subjects, each performing 12 attempts: 9 genuine attempts produced by three head motions (yaw, pitch, yaw+pitch) (see Fig. 4) with three different speeds (slow, medium, fast), and 3 spoofing attempts produced by the motion of a user photo (shift-rotation, bending, zoom). We underline that the experiments use specific moves just to have a well-defined test-bed and to better analyze classes of moves (simple, composite), but the system works with any move. Our system was also tested on two publicly available face database. The first is NUAA [15], with videos from 15 users, both live and in photo, captured in two sessions. During live recording the subject is still and simulates a photo; this is not suited to our experiments, since we try to catch the symmetric situation. As for the photos, the subject tries to simulate a real user by moving the photo (horizontally, vertically, back and front, rotating it in depth along the vertical or horizontal axis, bending it inward and outward along the vertical or horizontal axis). The second database is HONDA (training dataset) [8], with 20 video sequences, one for each user, captured at 15 fps with 640×480 resolution and with significant 2-D (in-plane) and 3-D (out-of-plane) head rotations. We further underline that results are convincing on the different real datasets, even if we left the whole configuration of parameters unchanged. In practice, the system does not need any training. We use 2 different datasets for either genuine or spoof requests. We considered this would not affect results: in this specific kind of attack, photos would always be submitted by impostors, never by genuines. We just want to discriminate 2D from 3D; testing of actual recognition would require a single dataset, but is a separate problem.

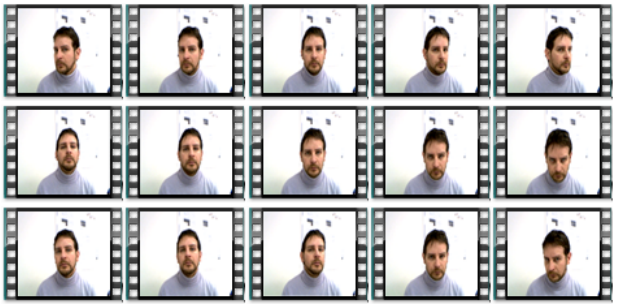

Fig. 4. Head motions: yaw(first row), pitch (second row), and yaw+pitch (third row).

In the first experiment the number *K* of frames in the *observation window*, is fixed to its maximum (25 frames). EER is measured for different combinations of movement and speed. Table 1 shows the results. We observe that a fast and articulated motion (yaw+pitch) makes the system well discriminative. This is an advantage in real settings. In fact, with yaw or pitch alone, some points, like the centre of eyes, just follow a linear horizontal or vertical path. More complex pose variations like yaw+pitch provide better results, since all face points follow an articulated path and generate greater deformations in the observed model. On the other hand, the speed of face movements is strictly correlated with the computation of variations of the cross ratio. If a true user moves face slowly, the values of the cross ratio change slowly and the variation computed in the observation window is quite low. With a fast movement, the cross ratio rapidly changes providing a higher variance. On the contrary, for a 2D surface (face photograph), values of the cross ratio remain almost constant, so the variance is very low in both cases.

Table 1 EER for varying motion type and speed, when K is 25.

| | yaw | pitch | yaw+pitch |
|---|---|---|---|
| Slow | 0.35 | 0.70 | 0.35 |
| Medium | 0.29 | 0.70 | 0.00 |
| Fast | 0.00 | 0.29 | 0.00 |

In the second experiment, motion is yaw+pitch, which gave the best results before; *K* as well as motion speed vary. Table 2 shows that with fast motion, a window of 10 frames only can provide a significantly good result.

Table 2 EER values with varying values of K parameter and of speed, for yaw+pitch motion.

| | 5 frame | 10 frame | 15 frame | 20 frame | 25 frame |
|---|---|---|---|---|---|
| Slow | 0.70 | 0.58 | 0.35 | 0.35 | 0.35 |
| Medium | 0.64 | 0.58 | 0.35 | 0.29 | 0.00 |
| Fast | 0.06 | 0.00 | 0.00 | 0.00 | 0.00 |

Fig. 5 shows the distributions of values for $v$ for genuine users (HONDA) and impostors (NUAA), with the same previous configuration of parameters ($K$=25, $th_j$=0.3, $th_v$=0.3). Time to process each frame, i.e. to locate face points and compute invariants, on a computer equipped with an Intel processor U7300 1.30Ghz and 4GB RAM is about 0.12s for a resolution of 800×600.

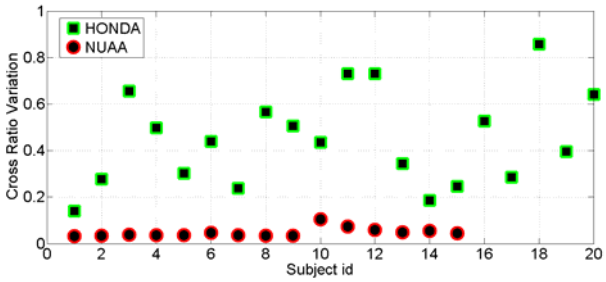


Fig. 5. $v_i$ for genuine (HONDA) and impostor (NUAA) users.

## 9. Conclusions

Spoofing is a weak point in face authentication, which is often not addressed. Literature presents a number of solutions, yet not free from limitations. Some of them only detect very simple attacks. Among the most robust methods, we mention those combining 3D verification and user interaction. In this work we presented a system in this category exploiting projective invariants. Our approach can verify if the face is truly 3D still maintaining a low computational cost. User interaction allows to also detect more complex spoofing such as the presentation of pre-recorded videos. Experiments show effectiveness and efficiency of the method. In the current implementation, the system could not detect spoofing via a 3D moving facial mask. A future work may include the fusion with further techniques such as eye blink or skin reflectance analysis to address this further problem, by implementing a multi-expert system. As a matter of fact, such fusion would help overcoming the limitations of single strategies. For example, eye-blink detection may be cheated by a mask which leaves visible both the eyes and eyebrows.

## Aknowledgements

Eurecom is a partner of TABULA RASA: "Trusted Biometrics under Spoofing Attacks". TABULA RASA is a project funded by the European Commission, under the Seventh Framework Programme.

## References

[1] P.N. Belhumeur, D.W. Jacobs, D.J. Kriegman, N. Kumar, N. Localizing parts of faces using a consensus of exemplars. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2011, pp. 545 – 552, June 2011

[2] J.B. Burns, R. Weiss, and E. Riseman, View Variation of Point-Set and Line Segment Features, in Proceedings Image Understanding Workshop, pp. 650-659, 1990.

[3] T. Choudhury, B. Clarkson, T. Jebara, A. Pentland, Multimodal person recognition using unconstrained audio and video, In Proc. of Int. Conf. on Audio- and Video-Based Biometric Person Authentication, pp.176–181, 1999.

[4] D. Forsyth, J. L. Mundy, A. Zisserman, C. Coelho, A. Heller, and C. Rothwell, Invariant Descriptors for 3-D Object Recognition and Pose, *IEEE Trans. PAMI*, vol. 13 n. 10, pp. 971–991, 1991.

[5] R. W. Frischholz, U. Dieckmann, BioID: A Multimodal Biometric Identification System, IEEE Computer, vol. 33, no. 2, pp.64–68, February 2000.

[6] K. Kollreider, H. Fronthaler, J. Bigun, Evaluating liveness by face images and the structure tensor, IEEE Work. on Automatic Identification Advanced Technologies, pp.75–80, 2005.

[7] K. Kollreider, H. Fronthaler and J. Bigun. Verifying liveness by multiple experts in face biometrics. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2008. CVPR '08, pp 1-6.

[8] K.-C. Lee, J. Ho, M.H. Yang, and D. Kriegman, Visual tracking and recognition using probabilistic appearance manifolds, Computer Vision and Image Understanding, no. 3, pp. 303–331, 2005.

[9] J. Li, Y. Wang, T. Tan, A. Jain, Live Face Detection Based on the Analysis of Fourier Spectra, Biometric Technology for Human Identification, Proc. SPIE, vol. 5404, pp. 296–303, 2004.

[10] S. Milborrow. Locating Facial Features with Active Shape Models. Master Thesis available at http://www.milbo.org/stasm-files/masters-milborrow-4.pdf

[11] S.Milborrow, F. Nicolls., Locating facial features with an extended active shape model, European Conf. Computer Vision, pp. 504–513, 2008.

[12] K. A. Nixon, V. Aimale, R. K. Rowe, Spoof Detection Schemes, in A.K. Jain, P. Flynn and A.A. Ross (eds.), Handbook of Biometrics, Springer, 2007.

[13] G. Pan, Z. Wu and L. Sun, Liveness Detection for Face Recognition, in Kresimir Delac, Mislav Grgic and Marian Stewart Bartlett (eds.), Recent Advances in Face Recognition, pp. 236, December 2008, I-Tech, Vienna, Austria.

[14] D. Riccio, J.-L. Dugelay, Geometric Invariants for 2D/3D Face Recognition, *PRL*, vol. 28, pp. 1907–1914, 2007.

[15] X.Tan, Y.Li, J.Liu and L.Jiang, Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model, in Proceedings of 11th European Conf. on Computer Vision (ECCV'10), Crete, Greece. September 2010.

[16] F. Tsalakanidou, C. Dimitriadis, S. Malassiotis. A secure and privacy friendly 2D+3D face authentication system robust under pose and illumination variations. Proc. of Eight International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS '07). p. 40 (Abstract)

[17] H. Wang; S. Z. Li, Y. Wang, and J. Zhang, Self quotient image for face recognition, International Conf. on Image Processing, pp. 1397-1400, 2004.