Shape Analysis Based Anti-spoofing 3D Face Recognition with Mask Attacks

Yinhang Tang(✉) and Liming Chen

Université de Lyon, Ecole Centrale de Lyon,
LIRIS laboratory UMR CNRS 5205, 69134 Lyon, France
tang-yinhang@doctorant.ec-lyon.fr

Abstract. With the growth of face recognition, the spoofing mask attacks attract more attention in biometrics research area. In recent years, the countermeasures based on the texture and depth image against spoofing mask attacks have been reported, but the research based on 3D meshed sample has not been studied yet. In this paper, we propose to apply 3D shape analysis based on principal curvature measures to describe the meshed facial surface. Meanwhile, a verification protocol based on this feature descriptor is designed to verify person identity and to evaluate the anti-spoofing performance on Morpho database. Furthermore, for simulating a real-life testing scenario, FRGCv2 database is enrolled as an extension of face scans to augment the ratio of genuine face samples to fraud mask samples. The experimental results show that our system can guarantee a high verification rate for genuine faces and the satisfactory anti-spoofing performance against spoofing mask attacks in parallel.

1 Introduction

As the most significant biometric trait of human beings, the human face has been widely used for human identification and verification in the scientific research and the real-world application. The facial data acquisition method is natural, non-intrusive and contactless, which is friendly to accept in social activities [11,12]. With the development of 3D scanner, 3D printer, Virtual Reality (VR) and Augmented Reality (AR), capturing and reconstructing 3D samples become more convenient in daily-life [30]. Meanwhile, 2D and 3D face recognition have been applied widely in the criminal investigation, the access control, the frontier inspection and the bank service. Even though the techniques of the face recognition have been widely studied in biometrics research area [1,2,9,19,26,36] and many state-of-the-arts have been reported in many publications, the spoofing attacks against face recognition systems is a potential threat to biometric application.

Spoofing attack is defined as an intrusive act of deceiving a biometric system by presenting a fake evidence or a copied biometric trait to obtain a valid authentication [28]. By using photographs or videos captured in distance or collected via internet, the attacker can easily achieve the facial information of a

B. Ben Amor et al. (Eds.): RFMI 2016, CCIS 684, pp. 41–55, 2017.
DOI: 10.1007/978-3-319-60654-5_4

valid user registered in a face recognition system. Then the attacker shows the fake photograph printed on paper or the recorded video displayed on a tablet for attempting to get access in the system. Furthermore, since few yeas ago, a social public website "Thats My Face"[1] started to provide the wearable 3D mask manufacturing service with only one frontal photo (another side-view photo is asked as option). It further reduced the difficulty of attacker's deception by wearing such a 3D printed mask. The simplicity and the convenience of the acquirement and the manufacture of the 2D/3D face data, which should be the advantages of the face recognition, become gradually the jeopardy and the calamity to the reliability and the stability of the face recognition system.

Due to the vulnerability of face recognition systems, many papers have been published on countermeasure studies, and the reported experimental results showed that the corresponding methods are sufficient and efficient. Among the published works, liveness detection [3,15,29,39], motion detection [5,14] and texture analysis [20,25] are three principal categories of anti-spoofing methods [6,7] against photo- and video-based spoofing attacks. However, with the help of the improvement of 3D manufacture technology, the easily obtained high-quality 3D masks introduce new challenge to anti-spoofing research. Morpho database[2] and 3DMAD database [6], including 2D, 2.5D and 3D face samples of genuine person and imposters wearing 3D mask, were constructed for simulating this mask intrusion. Kose *et al.* proposed the countermeasure based on the fusion of the information extracted from texture and depth images, and tested it on the Morpho database [16–18]. Erdogmus *et al.* evaluated various LBP based countermeasures on texture images in [6,7]. All of their works reported that the texture information can be essential discriminative characters to distinguish real faces and masks. However, the shape analysis based approach, as an important kind of methods in 3D face recognition, has not been discussed and studied in their works. To fill this gap, in this paper, we aims to evaluate the anti-spoofing performance of this kind of method.

The general technique of the shape analysis based 3D face recognition is to utilize the geometric attributes to describe and characterize the facial surface precisely. Geometry attributes, including principal curvatures, Gaussian curvature, mean curvature and their variations (e.g. shape index), have been commonly used to 3D face representation [21,22,35], keypoints location [24,26,38] and 3D facial feature descriptor generation [8,19,31]. In this study, we exploit "curvature measures" developed by [27,32,33] based on concept of normal cycle [4] to extract shape information of discrete surface (*e.g.* 3D meshed face), and design the corresponding facial description and recognition framework. This triangle mesh based geometric feature can highlight the micro-shape dissimilarity between genuine faces and manufactured masks, which leaves us more opportunities to distinguish them.

Besides, in the real-life scenario, comparing to the verification cases with genuine face samples, the spoofing mask attacks appear more rarely, which are

[1] http://www.thatsmyface.com.
[2] http://www.morpho.com.

regarded as an exceptional testing case. In order to simulate such a scenario, we firstly propose to combine Morpho database and FRGCv2 database [1], the largest public 3D face database, to appraise the anti-spoofing performance. The gallery set and the genuine probe set are formed by the genuine face samples coming from both Morpho database and FRGCv2 database, while the testing fake face scans from Morpho database are 5% and 1% of the scale of the whole probe set. This performance evaluation scenario corresponds better to the real-life case. Meanwhile, the conventional discriminative power evaluation and anti-spoofing performance test on Morpho database are also reported in the experiment part.

The rest of this paper is organized as follows. Section 2 gives a brief review of related anti-spoofing face recognition works. Section 3 presents principal curvature measures estimation method and the related shape analysis based facial feature descriptor. Section 4 shows the experimental results in several scenarios, and Sect. 5 finally concludes the paper.

2 Related Work

In the history of mask anti-spoofing research, the work of Kim *et al.* [13] can be regarded as the first published one. Due to the difference of the reflectance between face skin and materials used to manufacture mask, their work aimed to analyse the distribution of albedo values for illumination at various wavelengths. Based on Fisher's linear discriminant, they selected a 2D feature vector consisting of radiance measurement to be the classification criteria in visual and NIR spectrum (685 and 850 nm respectively). Similarly, Zhang *et al.* published their mask detection countermeasure based on multi-spectral analysis in [39]. They claimed to abandon visual face image, but to analyse multi-spectral images captured in two discriminative wavelengths of illumination (850 and 1450 nm). They measured the albedo curves of different materials and trained SVM classifier to distinguish real face and mask. Even though these two papers above are effective in mask distinguishing, they haven't resolve the anti-spoofing problem. Besides an extra multi-spectral capturing device is obligatory in their defence system.

Lately, Kose *et al.* reported their anti-spoofing works based on texture and depth information in 2D and 2.5D images from Morpho Database. Three baseline face recognition algorithms are tested and an anti-spoofing mask attack related experimental strategy is mentioned in [17]. Furthermore, they extracted LBP features in color and depth image and trained the linear SVM classifier to determine whether the input sample is genuine or fake in [16]. Then in order to combine the advantage of color and depth image in anti-spoofing mask attack, two feature and score level fusions were proposed in [18]. They concluded that texture analysis is a effective method for developing a countermeasure. Similarly, Erdogmus *et al.* introduced their 3D Mask Attack Database (3DMAD) and anti-spoofing countermeasures based on three extended LBP algorithms in [6]. Some more comparative anti-spoofing experimental results on Morpho and 3DMAD databases were reported in [7]. Even though the works presented above introduced great countermeasures against 3D mask attacks, all of their main methods

are designed based on 2D images projected from 3D face scans. Moreover their evaluation of the anti-spoofing capability of 3D face samples is constructed relying on Thin Plate Spline (TPS) warping parameters and Iterative Closest Point (ICP) methods. But 3D shape based geometric attributes, as potent characters in 3D shape analysis, haven't been evaluated their anti-spoofing potentiality. Besides, all their experiments are limited into the mask attack related database which doesn't includes not enough genuine face scans to test. In this paper, we have two main purposes to fill the gaps:

- We take full advantage of *principal curvature measures* based on asymptotic cone theory to design a facial descriptor, and evaluate the potential anti-spoofing performance of the facial descriptor for 3D meshed face scans.
- For simulating a real-life recognition case, we firstly attempt to combine a scale limited genuine-imposter combined database (*i.e.* Morpho database) to a large genuine face scans database (*i.e.* FRGCv2 database), and perform comprehensive experimental scenarios.

3 Principal Curvature Measures Based 3D Face Recognition Scheme

The shape analysis is regarded as an important kind of 3D face recognition methods. Among this branch of approaches, both a precise estimated geometric attribute and a proper related facial feature descriptor are significant to represent and describe the shape of facial surface. In this section, we will introduce our principal curvature measures estimation method and their related 3D face recognition scheme, which meet these two demands of this kind of method. Meanshile, because the surface of manufactured mask is smoother than real face which is stated in [17,18], our proposed descriptor, which can highlight the dissimilarity of the minor shape between genuine faces and masks, is capable to verify the liveness of the testing samples. The pipeline of our proposed method includes 4 steps: principal curvature measures estimation, 3D keypoint detection, 3D keypoint feature description and 3D keypoint matching.

3.1 Principal Curvature Measures Estimation

In general speaking, principal curvatures are the most basic but fundamental geometrical attributes in differential geometry. They are defined regularly as below: Suppose a point p locating on a smooth oriented surface S, its principal curvatures λ_{1_p} and λ_{2_p} are estimated as the eigenvalue sets of the corresponding second fundamental form h (q is the quadratic form associated to h). λ_{1_p} and λ_{2_p} can describe the local bending information around p of S. Remark that this definition is coherent because of the smoothness of surface S. However, 3D face sample is commonly recorded as the triangle mesh, which is continuous but piecewise smooth. It makes the conventional curvature estimation method unsuitable here. A possible solution proposed and demonstrated in [32,33] is to generalize

the definition of curvatures to the discrete surface and to replace functions by measures. Here we will present the generalization from the smooth surface case to the discrete surface case. Please refer [32,33] for a comprehensive and detailed introduction of the generalization.

Principal Curvature Measures of Smooth Surfaces. Inspiered to [32,33], the second fundamental form h and its associated quadratic form q can be generalized to a measure on a smooth surface S on $\mathbb{E}^3$. Suppose that any Borel subset B of $\mathbb{E}^3$ and any vector field X of $\mathbb{E}^3$, the definition of $\overline{h}_B$ and $\overline{q}_B$ are:

$$\begin{aligned} \overline{h}_B(X,X) &= \int_{S\cap B} h_p(pr_{T_pS}X_p, pr_{T_pS}X_p)dp, \\ \overline{q}_B(X) &= \int_{S\cap B} h_p(pr_{T_pS}X_p, pr_{T_pS}X_p)dp \\ &= \int_{S\cap B} q_p(pr_{T_pS}X_p)dp, \end{aligned} \tag{1}$$

where pr_{T_pS} denotes the orthogonal projection over the tangent plane T_pS of S at p. If X is a constant vector fields in $\mathbb{E}^3$, for any fixed Borel subset, $\overline{q}_B(X)$ is a measure. $\{\lambda_{1_B}, \lambda_{2_B}, \lambda_{3_B}\}$ is the associated eigenvalue set, and $\{e_{1_B}, e_{2_B}, e_{3_B}\}$ is the eigenvector set of $\overline{h}_B$. The map $\lambda_i : B \to \lambda_{i_B}, i \in \{1,2,3\}$ is a measure of $\mathbb{E}^3$, named as *principal curvature measure*. Remark that, in piece-wise case, principal curvature measures have three components rather than two in the point-wise approach.

Principal Curvature Measures of Triangle Meshes. A triangle mesh is a discrete surface apparently, which means its shape and bending information can not be describe by point-wise approach. That's why the measure theoretic method is coherent in triangle mesh case. According to the concept and theory of normal cycle [4,27], suppose a triangle mesh $\mathcal{T}$ in $\mathbb{E}^3$, an explicit formula of $\overline{h}$ and $\overline{q}$ defined of constant vector field X as:

$$\begin{aligned} \overline{h}_B(X,X) &= \sum_{e\in E} l(e\cap B)\angle(e) <X,e><X,e>, \\ \overline{q}_B(X) &= \sum_{e\in E} l(e\cap B)\angle(e) <X,e>^2. \end{aligned} \tag{2}$$

where E denotes the set of edge e of $\mathcal{T}$, $l(e\cap B)$ denotes length of e belongs to B, and $\angle e$ denotes the signed angle between unit normals n_1 and n_2 of incident facets f_1 and f_2 to e. Meanwhile, $\overline{h}_B$ associated matrix F_B is written as:

$$F_B = \sum_{e\in E} l(e\cap B)\angle(e) e\cdot e^t. \tag{3}$$

We similarly name the set of eigenvalues $\{\lambda_{1_B}, \lambda_{2_B}, \lambda_{3_B}\}$ of $\overline{h}_B$ is the *principal curvature measures* of $\mathcal{T}$ over B. The corresponding set of eigenvectors $\{e_{1_B}, e_{2_B}, e_{3_B}\}$ of $\overline{h}_B$ can also be estimated. Based upon the generalization of

$\overline{h}_B$, three eigenvectors are respectively two principal directions and one normal direction of X over B.

In summary, the set of principal curvature measures $\lambda_{1_B}, \lambda_{2_B}, \lambda_{3_B}$ is coherent to the geometrical properties of 3D face scans in triangle mesh and comprehensively suitable to describe facial surface. These principal curvature measures are the essential geometric attributes (*i.e.* the geometric feature) of our 3D keypoint descriptor presented in following parts.

3.2 λ_B Based 3D Keypoint Detection

In order to guarantee the scale invariance property of facial descriptor, our keypoint detection is inspired by Lowe's SIFT [23] and related works [19,31], but the difference of principal curvature measures are used to locate keypoints. We firstly construct the Gaussian scale space by smoothing the face scan in triangle mesh with a series of Gaussian kernel g_{σ_s} (σ_s denotes to different scales). Given a vertex v_i in a face scan, the facial surface adjacent becomes smoother by convolving g_{σ_s} over neighbour vertices v_j and v_i is updated to $v_{i_{\sigma_s}}$ as (4).

$$v_{i_{\sigma_s}} = \frac{\sum_{v_j \in N(v_i,1)} g_{\sigma_s}(v_i, v_j) \cdot v_j}{\sum_{v_j \in N(v_i,1)} g_{\sigma_s}(v_i, v_j)} \tag{4}$$

where $N(v_i, 1)$ denotes the set of vertices within 1-ring neighbourhood of v_i and Gaussian kernel g_{σ_s} is defined as

$$g_{\sigma_s}(v_i, v_j) = exp(-\|v_i - v_j\|^2 / 2\sigma_s^2). \tag{5}$$

We estimate principal curvature measures λ_{i_B} over each scale space of 3D facial surface as introduced in Sect. 3.1, and then compute the keypoint location criterion called Difference of Curvatutre (DoC), referring to Difference of Gaussian (DoG) in SIFT.

$$\delta(\lambda_i(B_{v_{\sigma_s}}) = \lambda_i(B_{v_{\sigma_s}}) - \lambda_i(B_{v_{\sigma_{s-1}}}), i = 1, 2, 3 \tag{6}$$

where δ denotes Difference of Curvature over B. If DoC associated to v_i is the extreme among 1-ring vertices around v_i in three scales σ_{s-1}, σ_s and σ_{s+1}, v_i is defined as a keypoint v_k and σ_s is its corresponding detection scale. The keypoints detected by three principal curvature measures separately are combined as one group for following 3D keypoint description.

3.3 λ_B Based 3D Keypoint Description

3D keypoint description can be divided into two parts. The first one is to assign a primary direction for improving the robustness to minor head pose change. The second part is to construct histograms of curvature measures based feature descriptor.

Primary Direction Determination. Let's suppose one keypoint v_k and its proper scale σ_s of a face scan F as before. The primary direction $\mathbf{d}_{v_k}$ associated to v_k is defined by the neighbour vertices $\mathcal{N}(v_k)$ within a geodesic disc of σ_s related radius R_{σ_s}:

$$\mathcal{N}(v_k) = \{v_j \in F | Dist(v_k, v_j) \leq R_{\sigma_s}\} \tag{7}$$

We first determine a plane TS_{v_k} orthogonal to the unit normal vector ξ_{v_k} of v_k, then project the unit normal vector ξ_{v_j} of v_j on TS_{v_k}. The primary direction of v_k is created by computing a Gaussian weighted histogram of 360 bins (1 bin per degree) on TS_{v_k}, and determined as the peak of the weighted direction histogram. Here the Gaussian weight is defined as:

$$\begin{aligned} w(v_k, v_j) &= mag(v_j) \cdot g_{\sigma_s}(v_k, v_j), \\ mag(v_j) &= \sqrt{\xi^x(v_j)^2 + \xi^y(v_j)^2}. \end{aligned} \tag{8}$$

HoC Based Feature Descriptor Representation. We construct the feature descriptor of a keypoint by using principal curvature measures estimated on a set of neighbor vertices. Following 2D daisy descriptor [37], all the neighbor vertices locating in 9 ovelapping circles $r_1, r_2, \cdots, r_9$ with a radius of $3.75\sigma_s$ around the keypoint support one keypoint feature descriptor. r_1 locates in the central part and its center is the keypoint here. Starting form the primary direction, other 8 circles around range along as clock-wise order (as shown in Fig. 1), and the distance from their center to the keypoint is $4.5\sigma_s$. This kind of daisy flower pattern descriptor simulates the functioning of human complex cells in visual cortex [10], and tends to be invariant to minor face transformation.

Then we build three histograms of three principal curvature measures (hoc_i) respectively in each circular region of $r_1, r_2, \cdots, r_9$. In each circular region, the value of i^{th} principal curvature measure are quantized equally to 8 bins and weighted by Gaussian kernel, and the standard deviation is assumed as the Euclidean distance between current point to corresponding center of circle. After that, we normalize and concatenate all three principal curvature measures related 27 histograms (*3 principal curvature measures* $\times$ *9 regions*) following this rule:

$$HOC = \{hoc_1^{r_1}, hoc_1^{r_2} \cdots hoc_1^{r_9}, hoc_2^{r_1}, hoc_2^{r_2} \cdots hoc_2^{r_9}, hoc_3^{r_1}, hoc_3^{r_2} \cdots hoc_3^{r_9}\} \tag{9}$$

HOC, denoting to *Histogram Of principal Curvature measures*, is the keypoint feature descriptor.

3.4 3D Keypoint Matching

For keypoint matching, we aim to find matched keypoint pairs based on *HOC* feature descriptor. Assume a keypoint $v_{k_i}^1$ belongs to first facial surface and the set of all keypoints $\{v_{k_j}^2\}$ in second facial surface. We estimate the angle set

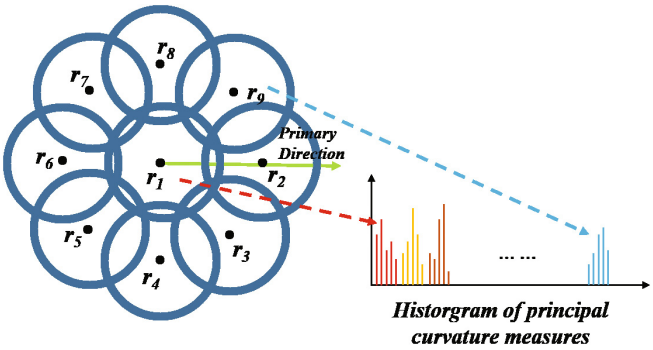

Fig. 1. Keypoint descriptor configuration in 9 overlapping circles for generating HoC.

$\{\alpha_j^i\}$ between feature vectors of $v_{k_i}^1$ and $\{v_{k_j}^2\}$ inspired to [31]. Each angle is defined as:

$$\alpha_j^i = cos^{-1}\left(\frac{< HOC_i^1, HOC_j^2 >}{||HOC_i^1|| \cdot ||HOC_j^2||}\right). \tag{10}$$

The angles α_j^i are then ranked in ascending order. If the ratio between the first and second angle is smaller than predefined threshold r_α, the match is accept. Otherwise it is rejected. Finally the number of matching keypoints is set as the similarity measurement μ between two facial surfaces.

4 Experiments

4.1 Database

In the experiment part, Morpho database and FRGC database are both involved for evaluation in different scenarios. We will introduce them briefly as follow.

Morpho Database. In Morpho databse, 16 masks were manufactured according to the facial information of 16 persons. Their faces are captured by 3D scanner with the structured light, and the mask is manufactured with 3D printer by Sculpteo 3D Printing [16]. Morpho database consists of two parts: (a) 20 subjects with 10 genuine face samples; (b) 20 subjects wearing their own or other's mask are captured around 10 times. In part (b), a person wearing his/her own mask is marked as a type A_A mask sample. Otherwise it's marked as a type A_B mask sample. In the following experiments, both A_A and A_B samples are both regarded as spoofing mask attacks. Some examples in Morpho database are shown in Fig. 2.

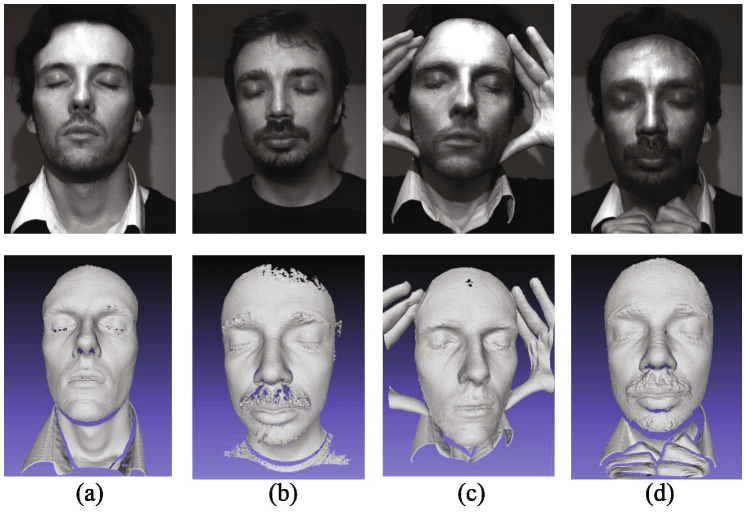

Fig. 2. 2D texture image and corresponding 3D mesh sample in Morpho database. (a) genuine face scan of person A; (b) genuine face scan of person B; (c) person A wears his own mask (type A_A fake sample); (d) person A wears person B's mask (type A_B fake sample).

FRGC V2.0 Database. FRGCv2 database is the largest published 3D face database, which is built with 4,007 3D face scans of 466 subjects with various facial expressions, genders and ages. All the face samples recorded are genuine faces. The face samples are captured in controlled pose and lighting condition by Minolta Vivid 900 scanner. After preprocessing step following [34], ROI contains about 30,000 vertices and 40,000 facets.

4.2 Experiment Scenarios

The basic purpose of our 3D face verification system is to guarantee the verification accuracy for genuine face, and the complementary purpose is to distinguish faces and masks. We hence firstly define a series of threshold of the similarity measurement t_μ^i in a baseline estimation scenario, and then we apply the same series of thresholds to evaluate the anti-spoofing performance of our facial feature descriptor. Furthermore, we also try to control the quantity ratio of genuine faces to fake faces in probe set for simulating a real-life case. Based on this idea, two series of experiment scenarios (Scenario A and B) are designed. For introducing clearly in following part, G_M and S_M denotes respectively to the set of all genuine face scans and the set of all spoofing mask scans (including type A_A and A_B mask scans) in Morpho database. G_F denotes to the group of all genuine face scans in FRGC database. G_{M1} and G_{Mi} represents respectively the group of the first scan of individuals, and other samples of individuals in G_M (similarly for G_F).

- **Scenario A-1:** Baseline evaluation with Morpho database.
  G_{M1} forms *gallery set*, and G_{Mi} builds *probe set*.
- **Scenario A-2:** Anti-spoofing performance evaluation with Morpho database.
  G_{M1} forms *gallery set*, and G_{Mi} and S_M build respectively *probe set* and *spoofing probe set*.
- **Scenario B-1:** Baseline evaluation simulating real-life case.
  G_{M1} and G_{F1} build *gallery set*, and G_{Mi} and G_{Fi} build *probe set*.
- **Scenario B-2:** Simulating real-life case including 5% fake scans against 95% genuine face scans.
  G_{M1} and G_{F1} build *gallery set*, G_{Mi} and G_{Fi} build genuine face *probe set*. S_M build *spoofing probe set*.
- **Scenario B-3:** Simulating real-life case including 1% fake scans against 99% genuine face scans.
  Gallery set and genuine face probe set is same as B-2, but only 20% scans of S_M enrolled in *spoofing probe set*. The quantity ratio between fake scans and genuine face scans is 1:99.

4.3 Experimental Results and Analysis

In scenarios A-1 and B-1, we evaluate the baseline of verification performance with True Accept Rate (TAR). Because TAR varies along with t_μ^i, TAR is shown in Table 1 under several False Accept Rate (FAR) cases. For scenarios A-2, B-2 and B-3 in Table 1, we first take only spoofing probe set to evaluate the anti-spoofing performance. Recall it that all scans in spoofing probe set are type A_A or A_B mask scans which are treated as illegal samples and should be rejected by system. True Accept Rate (TAR) and False Reject Rate (FRR), which are commonly used as criterion, can't be estimated in this case, because there are only two verification results for the spoofing probe sample, which are accepted falsely (FAR) or rejected correctly (TRR). Therefore we evaluate the performance with *Spoofing True Reject Rate* (STRR) as criterion for spoofing scans in scenarios A-2, B-2 and B-3 with FAR predefined in scenario A-1 and B-2 respectively. STRR is a special criteria for the spoofing samples, so as to show the distinction to TRR for the genuine face samples.

As shown in Table 1, the verification rate in baseline evaluation with Morpho Database is above 92% except the case that FAR is 0.01. And in real-life simulating case, we extend the scale of database by adding FRGC database and the verification rate is 91.98% even FAR equals only 0.001. If FAR is 0.01, the TAR increases from 84.75% to 94.68% which means the real-life simulating scenario with more samples can evaluate more properly the performance. Here, we can conclude that, in the baseline evaluation scenarios, our 3D face feature guarantees the verification performance for only genuine faces. Even though TAR is 84.75% in A-1, it can't deny the above conclusion. Because the scale of genuine face scans in A-1 is 180, which means there are only 1 or 2 samples accepted falsely if FAR is 0.01. And that's why we don't show the results of A-1 and A-2 when FAR is 0.001. By the way, based on the contrary thought, the results when FAR is 0.1 are blank in last three scenarios. Because there are 3,721 genuine face

Table 1. Verification and anti-spoofing performance evaluation in scenarios

Scenarios	A-1	A-2	B-1	B-2	B-3
FAR	TAR	STRR	TAR	STRR	STRR
0.1	94.35%	62.82%	-	-	-
0.05	92.09%	69.49%	96.41%	62.97%	69.49%
0.01	84.75%	75.64%	94.68%	73.59%	73.78%
0.001	-	-	91.98%	81.28%	84.59%

scans in scenario B-1, and if FAR is 0.1, there are too many samples accepted falsely which can't show the performance correctly.

In scenario A-2, STRR is above 62.82% and arrives 75.64% when FAR is 0.01. It's obvious that our algorithm can distinguish the genuine face and fraud mask from Morpho database. STRR arises along with decrease of FAR because threshold t_μ^i is more restricted. Moreover, in real-life simulating case, STRR is higher than 62.97% and achieves 81.28% and 84.59% including different spoofing probe set. In this case, STRR is lower a bit with same FAR than A-2 because the scale of gallery set is larger and t_μ^i is more rough. However, this experimental results also demonstrate our algorithm can complete the anti-spoofing mission even the mask manufactured in high quality.

After that, for scenarios A-2, B-2 and B-3, we combine genuine face related probe set (G_{Mi} and G_{Fi}) and spoofing probe set (S_M) to evaluate the performance. Here a Detection Error Trade-off graph (DET) is given to show the experimental results (as shown in Fig. 3). Remark that in order to present clearly, the figure only shows the part when FAR and FRR is lower than 35% in scenarios B. In Fig. 3, the lower Equal Error Rate (ERR) is, with same gallery set, the better verification performance is. In this DET graph, when the scale of gallery set is limited in Morpho database, EER of A-2 is 9.3% higher than the baseline. It's obvious to study that the involvement of spoofing mask samples decreases the verification rate in scenarios A. In similar, when we extend the scale of gallery set enrolling FRGC database, EER of B-2 and B-3 is higher than corresponding baseline experiment. But comparing to A-2, EER declines to 3.1% and 2.8%. A similar conclusion obtained as before that two goals have been achieved: (1) the verification system guarantees a high verification ability and (2) it possesses the distinguishable power against spoofing attack in real-life simulating case.

4.4 Comparison with the State-of-the-Art Approaches

In this subsection the comparison with the state-of-the-art approaches using Morpho database is also given in Table 2. According to the experimental configuration assigned in [7,17], here we use scenario A-1 to compute the EER. Then adopt the same threshold in A-2 to compute the SFAR, that is, *Spoofing False Accept Rate*. Spoofing False Accept indicates to the case that the samples with mask is false accepted by the sysem. In Table 2, we only report our experimental

Table 2. Comparison of verification performance with spoofing attacks in Morpho database. (1) Results reported in [17], (2) results reported in [7], (3) results with our proposed method.

	Texture Image		Depth Image		3D Mesh Model		
	(1)	(2)	(1)	(2)	(1)	(2)	(3)
EER	5.90%	6.54%	7.27%	17.63%	3.85%	9.58%	6.72%
SFAR	72.87	59.94%	88.94	47.98%	91.46	54.09%	33.10%

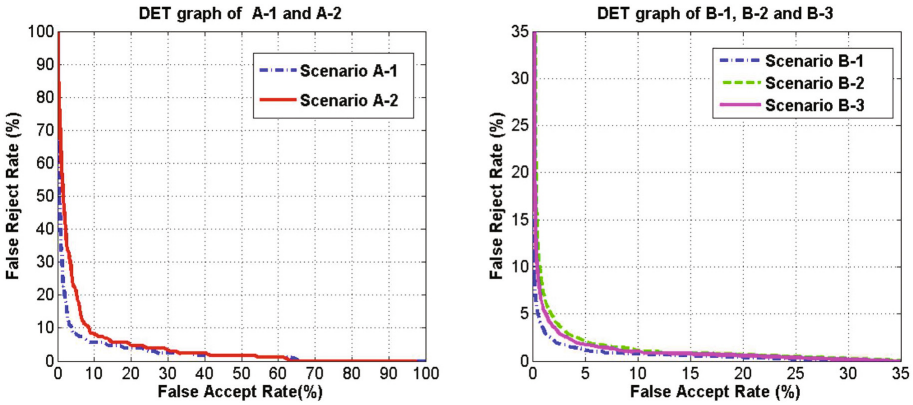

Fig. 3. Detection error trade-off graph of experimental scenarios: Scenarios A-1 and A-2 are shown in left graph, Scenarios B-1, B-2 and B-3 are shown in right graph.

results using 3D mesh samples. Comparing to 2D texture image and 2.5D depth image, the face recognition based on 3D face samples generally achieve higher verification performance with all genuine face samples in the test. The warping parameters related method in [17] achieves the lowest EER of 3.85%, which is better than 6.91% EER obtained by our method. However, the WP-related FR system is the most vulnerable one among the reported systems. Our PCM-meshSIFT-based method is the most robust system when replace all the probe samples by the samples with masks. We achieve the lowest SFAR of 33.10% in such experiment. It proves that the minor shape difference between genuine faces and manufactured masks can be detected and highlighted by our principal curvature measure based 3D facial feature, which is effective to enhance the security level of FR system.

5 Conclusion

In this paper, we first propose to using 3D shape description related method to distinguish the genuine faces and the spoofing masks stored in 3D triangle meshes. Due to the estimation process relying on a integral form, principal curvature measures are suitable to present the shape of triangle mesh directly.

Furthermore, principal curvature measures related feature descriptor can characterize properly the shape information of facial surface, and highlight the minor dissimilarity of shape between manufactured masks and genuine faces. Thereby our system can guarantee both high verification rate for genuine face and satisfactory anti-spoofing performance against mask attack.

Moreover, in a real-life case, the spoofing mask attack is a small proportion of testing samples. In experiment part, we hence propose to extend the probe set by combining mask samples in Morpho database and genuine faces in FRGCv2 database for simulating a real-life verification environment. The experimental results show that our method is effective in verification scenario and anti-spoofing performance during this simulating case.

Acknowledgements. This work was supported in part by the French research angency, l'Agence Nationale de Recherche (ANR), through the Biofence project under the grant **ANR-13-INSE-0004-02**.

References

1. Bowyer, K.W., Chang, K., Flynn, P.: A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition, vol. 101, pp. 1–15. Elsevier (2006)
2. Bronstein, A.M., Bronstein, M.M., Kimmel, R.: Expression-invariant 3D face recognition. In: Kittler, J., Nixon, M.S. (eds.) AVBPA 2003. LNCS, vol. 2688, pp. 62–70. Springer, Heidelberg (2003). doi:10.1007/3-540-44887-X_8
3. Chetty, G., Wagner, M.: Multi-level liveness verification for face-voice biometric authentication. In: 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, pp. 1–6. IEEE (2006)
4. Cohen-Steiner, D., Morvan, J.M.: Restricted delaunay triangulations and normal cycle. In: ACM, pp. 312–321 (2003)
5. De Marsico, M., Nappi, M., Riccio, D., Dugelay, J.L.: Moving face spoofing detection via 3D projective invariants. In: 5th IAPR International Conference on Biometrics, pp. 73–78. IEEE (2012)
6. Erdogmus, N., Marcel, S.: Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect. In: IEEE International Conference on BTAS, pp. 1–6 (2013)
7. Erdogmus, N., Marcel, S.: Spoofing face recognition with 3D masks. IEEE Trans. Inf. Forensics Secur. **9**(7), 1084–1097 (2014)
8. Gordon, G.G.: Face recognition based on depth and curvature features. In: IEEE Computer Society Conference on CVPR, pp. 808–810 (1992)
9. Huang, D., Ardabilian, M., Wang, Y., Chen, L.: 3-D face recognition using elbp-based facial description and local feature hybrid matching. IEEE Trans. Inf. Forensics Secur. **7**(5), 1551–1565 (2012)
10. Hubel, D.H., Wiesel, T.N.: Receptive fields, binocular interaction and functional architecture in the cat's visual cortex. J. Physiol. **160**(1), 106–154 (1962)
11. Jain, A., Hong, L., Pankanti, S.: Biometric identification. Commun. ACM **43**(2), 90–98 (2000)
12. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)

13. Kim, Y., Na, J., Yoon, S., Yi, J.: Masked fake face detection using radiance measurements. JOSA A **26**(4), 760–766 (2009)
14. Kollreider, K., Fronthaler, H., Bigun, J.: Evaluating liveness by face images and the structure tensor. In: IEEE Workshop on Automatic Identification Advanced Technologies, pp. 75–80 (2005)
15. Kollreider, K., Fronthaler, H., Bigun, J.: Verifying liveness by multiple experts in face biometrics. In: IEEE Computer Society Conference on CVPRW, pp. 1–6 (2008)
16. Kose, N., Dugelay, J.L.: Countermeasure for the protection of face recognition systems against mask attacks. In: 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), pp. 1–6. IEEE (2013)
17. Kose, N., Dugelay, J.L.: On the vulnerability of face recognition systems to spoofing mask attacks. In: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 2357–2361. IEEE (2013)
18. Kose, N., Dugelay, J.L.: Shape and texture based countermeasure to protect face recognition systems against mask attacks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 111–116 (2013)
19. Li, H., Huang, D., Morvan, J.M., Wang, Y., Chen, L.: Towards 3D face recognition in the real: a registration-free approach using fine-grained matching of 3D keypoint descriptors. Int. J. Comput. Vision **113**(2), 128–142 (2015)
20. Li, J., Wang, Y., Tan, T., Jain, A.K.: Live face detection based on the analysis of fourier spectra. In: Defense and Security, pp. 296–303 (2004)
21. Li, X., Jia, T., Zhang, H.: Expression-insensitive 3D face recognition using sparse representation. In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 2575–2582 (2009)
22. Li, X., Zhang, H.: Adapting geometric attributes for expression-invariant 3D face recognition. In: IEEE International Conference on Shape Modeling and Applications, pp. 21–32 (2007)
23. Lowe, D.G.: Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vision **60**(2), 91–110 (2004)
24. Lu, X., Jain, A.K., Colbry, D.: Matching 2.5D face scans to 3D models. IEEE Trans. Pattern Anal. Mach. Intell. **28**(1), 31–43 (2006)
25. Määttä, J., Hadid, A., Pietikäinen, M.: Face spoofing detection from single images using micro-texture analysis. In: International Joint Conference on Biometrics, pp. 1–7. IEEE (2011)
26. Mian, A., Bennamoun, M., Owens, R.: An efficient multimodal 2D–3D hybrid approach to automatic face recognition. IEEE Trans. Pattern Anal. Mach. Intell. **29**(11), 1927–1943 (2007)
27. Morvan, J.M.: Generalized Curvatures. Springer, Heidelberg (2008)
28. Nixon, K.A., Aimale, V., Rowe, R.K.: Spoof detection schemes. In: Jain, A.K., Flynn, P., Ross, A.A. (eds.) Handbook of Biometrics, pp. 403–423. Springer, New York (2008)
29. Pan, G., Sun, L., Wu, Z., Lao, S.: Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In: 11th IEEE International Conference on Computer Vision, pp. 1–8 (2007)
30. Pears, N., Liu, Y., Bunting, P. (eds.): 3D Imaging, Analysis and Applications, vol. 3. Springer, London (2012)
31. Smeets, D., Keustermans, J., Vandermeulen, D., Suetens, P.: meshSIFT: local surface features for 3D face recognition under expression variations and partial data. Comput. Vis. Image Underst. **117**(2), 158–169 (2013)

32. Sun, X., Morvan, J.M.: Curvature measures, normal cycles and asymptotic cones. Actes des rencontres du C.I.R.M. **3**(1), 3–10 (2013)
33. Sun, X., Morvan, J.M.: Asymptotic cones of embedded singular spaces. arXiv preprint arXiv:1501.02639 (2015)
34. Szeptycki, P., Ardabilian, M., Chen, L.: A coarse-to-fine curvature analysis-based rotation invariant 3D face landmarking. In: 3rd IEEE International Conference on Biometrics: Theory, Applications, and Systems, pp. 1–6 (2009)
35. Tanaka, H.T., Ikeda, M., Chiaki, H.: Curvature-based face surface recognition using spherical correlation. Principal directions for curved object recognition. In: 3rd IEEE International Conference on FG, pp. 372–377 (1998)
36. Tang, Y., Sun, X., Huang, D., Morvan, J.M., Wang, Y., Chen, L.: 3D face recognition with asymptotic cones based principal curvatures. In: IEEE International Conference on Biometrics, pp. 466–472 (2015)
37. Tola, E., Lepetit, V., Fua, P.: DAISY: an efficient dense descriptor applied to wide-baseline stereo. IEEE Trans. Pattern Anal. Mach. Intell. **32**(5), 815–830 (2010)
38. Wu, Z., Wang, Y., Pan, G.: 3D face recognition using local shape map. In: IEEE International Conference on Image Processing, vol. 3, pp. 2003–2006 (2004)
39. Zhang, Z., Yi, D., Lei, Z., Li, S.Z.: Face liveness detection by learning multispectral reflectance distributions. In: IEEE International Conference on Automatic Face & Gesture Recognition and Workshops, pp. 436–441 (2011)