MASK SPOOFING IN FACE RECOGNITION AND COUNTERMEASURES

Neslihan Kose, Jean-Luc Dugelay

MASK SPOOFING IN FACE RECOGNITION AND COUNTERMEASURES

Neslihan Kose, *Student Member, IEEE*, Jean-Luc Dugelay, *Fellow, IEEE*
Multimedia Department EURECOM Sophia-Antipolis France

Abstract

In this paper, initially, the impact of mask spoofing on face recognition is analyzed. For this purpose, one baseline technique is selected for both 2D and 3D face recognition. Next, novel countermeasures, which are based on the analysis of different shape, texture and reflectance characteristics of real faces and mask faces, are proposed to detect mask spoofing. In this paper, countermeasures are developed using both 2D data (texture images) and 3D data (3D scans) available in the mask database. The results show that each of the proposed countermeasures is successful in detecting mask spoofing, and the fusion of these countermeasures further improves the results compared to using a single countermeasure. Since there is no publicly available mask database, studies on mask spoofing are limited. This paper provides significant results by proposing novel countermeasures to protect face recognition systems against mask spoofing.

Keywords: spoofing, mask attacks, countermeasure, face recognition

Email address: neslihan.kose@eurecom.fr, jean-luc.dugelay@eurecom.fr (Neslihan Kose, *Student Member, IEEE*, Jean-Luc Dugelay, *Fellow, IEEE*)

1. INTRODUCTION

In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain access to recognition system. Face recognition is used in domains such as surveillance and access control. Since face data can be acquired easily in a contactless manner, spoofing is a real threat for face recognition systems.

The most common spoofing attacks are photograph and video attacks due to their convenience and low cost. Based on the observations that 2D face recognition (FR) systems are vulnerable to these attacks, researchers started to work on countermeasures to reduce their impact on recognition performances.

Proposed countermeasures against photo and video attacks are mainly based on liveness detection, motion analysis and texture analysis. Countermeasures based on liveness detection examine movements such as eye blinking [24] or lip movements [9]. In the literature, there are several countermeasures based on motion analysis [4, 22]. These countermeasures rely on the fact that the movement of a 2D plane is different compared to the movement of a 3D object. In [4], under the assumption that the test region is a 2D plane, the authors obtain a reference field from the actual optical flow field data. Then the degree of differences between the two fields is used to distinguish between a 3D face and a 2D photograph. In [22], a set of facial points are located automatically and their geometric invariants are used to detect attacks. The last

group is countermeasures based on texture analysis. In [3] and [19], images are examined to find printing artifacts and blurring, respectively. In [14], different contrast and texture characteristics of photographs and real faces are analyzed to detect spoofing. Furthermore in [20, 21], micro-texture analysis is proposed to detect 2D attacks. The study [7] includes brief information about different types of 2D face countermeasures, which were developed for a competition on countermeasures against 2D facial spoofing attacks. Six teams participated to this competition. These teams are AMILAB, CASIA, IDIAP, SIANI, UNICAMP and UOULU. All teams used one or multiple clues obtained clearly from motion analysis, texture analysis and liveness detection. The CASIA team presented a method with the combination of motion and texture analysis techniques, and the method also allows switching between detection schemes based on the scene context. The AMILAB and the UNICAMP teams used all motion analysis, texture analysis and liveness detection in deriving the detection scheme. IDIAP and UOULU used texture analysis method and obtained zero percent Equal Error Rate (EER) on development set and zero percent Half Total Error Rate (HTER) on test set. This leads to the conclusion that, the attack videos in the database used for this competition (i.e. PRINT-ATTACK Database [26]) mainly consist of detectable texture patterns.

When 3D masks are introduced as attacks, some of the countermeasures proposed for the detection of 2D attacks are no longer applicable. The study of Kollreider et al. [13] shows that a face recognition system relying on eye

blinking and lip movements can be defeated by using photographic masks wrapped over face with eyes and mouth regions cut out. Also, since motion based countermeasures depend on different movements of 2D and 3D surfaces, they are not applicable when masks are used instead of photos or videos. It appears that the detection of 3D mask attacks is more challenging compared to the detection of 2D facial attacks.

3D mask attacks to FR systems is a considerably new subject. The main reason for the delay in mask spoofing studies is due to the unavailability of public mask databases. To our knowledge, in the literature, there are two countermeasure studies against 3D mask attacks [11, 29] excluding our studies. These two studies are based on reflectance analysis. They utilize 2D data (texture images) in their approach to detect 3D mask attacks. Kim et al. [11] exploit the reflectance disparity based on albedo between real faces and mask materials (silicon, latex or skinjell). The feature vector, which is used in their approach for mask detection, consists of radiance measurements of the forehead region under 850 and 685 nm illuminations. They report 97.78% accuracy for mask detection. In [11], the experiments are done directly on the mask materials not on the real facial masks. Thus, it is not possible to report spoofing performances of the masks used. The measurements are done at exactly 30 cm and on the forehead region for mask detection. The requirement for an exact distance and occlusion possibility in the forehead during the measurements are the limitations of this method. In [29], multi-spectral reflectance analysis is proposed. After measuring the albedo curves of facial

skin and mask materials with varying distances, two discriminative wavelengths (850 and 1450 nm) are selected. Finally, a Support Vector Machine (SVM) [8] classifier is used to discriminate between real and fake samples. Experiments are conducted on a database of 20 masks from different materials (4 plastic, 6 silica gel, 4 paper pulp, 4 plaster and 2 sponge). The results show that this method can achieve 89.18% accuracy. The superiorities of [29] compared to [11] are the elimination of range limitation and the usage of real facial masks. However, spoofing performances of the masks are still not reported. In order to contribute to this compelling research problem and fill the missing portions of the existing studies, we have proposed several countermeasure techniques against 3D mask attacks in [15], [18] and [17].

The spoofing performances of the masks used and the countermeasure which uses 3D data (3D scan) instead of 2D data (texture image) as input to detect mask spoofing were first analyzed in our previous studies [16, 15], respectively, using the mask database which was prepared within the context of the European Union (EU) research project TABULA RASA [28]. The mask database used in the present study and our previous studies [15, 16, 18, 17] was created by MORPHO [23]. This database includes many high-quality mask samples. It consists of 3D masks of 16 real subjects. The scans of subjects were acquired by a 3D scanner, and the masks were manufactured using a 3D printer. In addition to texture images, it includes 3D scans for both real and mask samples. Thanks to the nature of this database, we were able to evaluate the impact of mask spoofing on both 2D and 3D face

recognition, and to develop our countermeasures using both 2D and 3D data.

If a 3D mask is not able to spoof a recognition system, it is not a successful attack, and there is no need to develop a countermeasure against it. Therefore, in [16], we analyzed how well the spoofing performances of the masks used in our studies are. The results of this study show that the masks used have very similar texture and especially 3D face shape characteristics to their target faces. They are very successful to spoof face recognition systems. To the best of our knowledge, spoofing performances of the masks used were the first to be analyzed in this study. In [15], we proposed to apply micro-texture analysis on both texture and depth images, and obtained 88.12% and 86% accuracy, respectively, for the classification of mask and real faces. The novelty of this work is that it was the first time 3D data was utilized to discriminate mask and real samples. In our next study [18], which is the continuation of [15], we studied fusing the information extracted from both the texture and depth images, and obtained a higher classification accuracy of 93.5%. In addition to the increase in performance, it was the first time the performances of face recognition systems were analyzed with/without mask attacks and with/without the proposed countermeasure integrated to the recognition systems in [18]. By this way, it is possible to observe the positive impact of countermeasure on recognition performances in presence of mask attacks. Finally, in [17], we proposed a countermeasure based on reflectance analysis using the texture images in the same database. We obtained 94% classification accuracy in [17], which was the best score we had obtained so

far.

In this paper, after showing the impact of attacks on the selected recognition systems; we provide an overview on our spoofing detection approaches which were introduced in the studies [15], [18] and [17]. We extend the works explained in these studies with some improvements, additional analysis, comparisons of performances of diverse countermeasures using the same protocol, and with a detailed analysis of the fusion scenarios. Additionally, a novel countermeasure is proposed in the present paper. In [15], micro-texture analysis is applied on texture images, whereas in this paper, we apply micro-texture analysis on reflectance components of texture images as a new countermeasure. We observe that higher accuracy is obtained using reflectance component instead of texture image (original image) itself. This proves that reflectance image provides more appropriate information than original image to discriminate mask and real samples. In the present study, we obtain 98.99% classification accuracy, which is the best accuracy that have been reported in the literature for mask spoofing detection up to now. Also, in the present paper, we integrate the countermeasure with the best performance to the selected 3D FR system in order to show the positive impact of the countermeasure on the system under mask attacks, directly.

The paper is organized as follows: Section 2 gives brief information on the mask database which is used in this study. Section 3 presents the selected 2D and 3D FR systems, and then evaluates the impact of mask spoofing on these systems. Section 4 gives brief information about the techniques that were

used to develop the proposed countermeasures. Section 5 explains each of the proposed countermeasures. Section 6 shows the experiments and results of all the proposed countermeasures together with the fusion scenarios for comparison purposes. Finally, conclusions are provided in Section 7.

2. THE MASK DATABASE

A mask used for 3D face spoofing purposes has to show very similar 3D shape characteristics to the target face to be considered as a successful attack. The mask database used in this study was prepared to fulfill this objective. Initially, scans of the subjects in the mask database were taken by a 3D scanner which uses a structured light technology in order to obtain similar face shape characteristics to the target person. Then the 3D model (3D mesh) of each subject was sent to a 3D printer and the masks were manufactured by Sculpteo 3D Printing [27]. The material used for the masks is polychrome mineral powder, which is a 3D printing standard.

The mask database is 2D+3D. For the sake of clarity, the database of real faces in 2D and 3D will be referred as DB-r2 and DB-r3, while the database of mask attacks will be referred as DB-m2 and DB-m3 in the rest of this paper.

In the mask database, 20 subjects appear in total. The masks were manufactured for 16 of these subjects. For DB-r, an average of 10 scans of each subject were acquired. For DB-m, an average of 10 scans of each subject wearing either his/her own mask or masks of the other subjects that

Figure 1: Example from the mask database which is created by [23]. From left to right (upper row) The real face, the cropped texture image, the 3D scan after preprocessing, the cropped depth map estimated from the raw 3D scan (lower row) same images for the corresponding mask attack.

appear in the same database were acquired. Finally, 200 real face acquisitions from 20 subjects and 198 mask acquisitions from 16 masks are used for the evaluations of this study. Figure 1 shows one example from this database for a real face access and the corresponding mask attack access.

In the mask database, DB-r and DB-m are partitioned in train and test sets. 8 subjects out of 16 subjects whose masks are manufactured, and 2 subjects out of 4 subjects whose masks are not manufactured are selected for DB-r. The samples of the selected subjects are assigned to the test set of DB-r, while the rest is used for the train set of DB-r. For DB-m, the mask attack accesses to the corresponding identities in the test set of DB-r are involved in the test set of DB-m, while the rest is used for the train set of DB-m. There is no overlap between the train and test sets, which makes the spoofing detection more challenging. Finally, there are 100 samples in each of the client (real accesses) test and train sets, and 99 samples in each of the

impostor (mask attack accesses) test and train sets.

3. IMPACT ANALYSIS OF MASK SPOOFING ON FACE RECOGNITION

In this section, initially, we explain the pre-processing applied for the selected 3D and 2D FR techniques. Next, we give the details about these recognition techniques. Finally, we evaluate the impact of spoofing mask attacks on both 3D and 2D face recognition.

3.1. Pre-Processing for the Selected Face Recognition Systems

The pre-processing for the selected 3D FR system is based on the method given in [10]. In order to crop the face region, the tip of the nose is detected, and the facial surface is cropped by a sphere with radius 80 mm, centered 10 mm away from the nose tip in +z direction. Note that the face looks towards +z direction. Next, the spikes are removed by thresholding, and then a hole filling procedure is applied. Finally, a bilateral smoothing filter is used to remove white noise while preserving edges. These pre-processed 3D scans (only shape, without texture) are used as input for 3D face recognition.

For 2D face recognition, the texture images in the mask database are cropped as shown in Figure 1, and resized into 64×64 images. In this study, we aim to show first how vulnerable the systems are to spoofing mask attacks by evaluating the performances of the selected systems with/without attacks, and then how a countermeasure improves the performance in presence of

mask attacks by evaluating the performances of these systems with/without countermeasure. For micro-texture analysis applied inside the proposed countermeasures, which is explained in Section 4, images are resized into 64×64 as proposed in [20]. Thus, although this resizing parameter may reduce the baseline performance in 2D, since our aim in this study is not to report high baseline performance, we preferred to use the same images as input for both the 2D baseline evaluation and proposed countermeasures.

Figure 1 shows an example for the texture images and 3D scans which are used in 2D and 3D evaluations, respectively.

3.2. Selected Face Recognition Systems

The 3D FR system selected as baseline for this study is introduced in [10]. It is also selected as baseline system in TABULA RASA project [28]. It uses the pre-processed 3D mesh of the face as input. Three landmark points are previously annotated at the nose tip and outer eye corners for each sample in the database. Initially, a linear transformation is computed in a least squares sense (LSS), based on two sets of landmarks (landmarks of generic model and subject's face). Least squares means that the overall solution minimizes the sum of the squares of the errors made in the results of every single equation. The best fit in the LSS here is calculated by minimizing the squared distance between the point sets of generic model and subject's face. For this purpose, the obtained transformation that includes rotation, translation and isotropic scaling is applied onto the generic model, aligning it

with the subject's face. Next, the alignment is further improved by Iterative Closest Point (ICP) method [5]. Afterwards, 140 previously selected points on the generic model are coupled with the closest vertices on the face under analysis, and Thin Plate Spline (TPS) [6] warping is applied on the generic model resulting in warping parameters (WP) of size 140×3. WPs that represent the deviations from the common structure are given to the classifier for recognition. Finally, the distance between two face models is computed by taking the median of cosine distances between the corresponding feature vectors (WP), and recognition rates are computed. Figure 2 shows the feature extraction scheme on a sample model using this method, which is named WP.

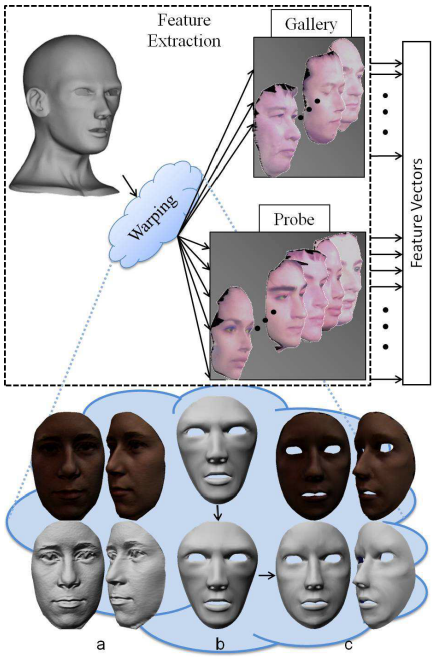


Figure 2: The feature extraction scheme and an illustration on a sample model: (a) The subject's face with and without texture (b) generic model before and after alignment (c) generic model after warping with and without texture. This figure is taken from [10].

For 2D face recognition, Local Binary Patterns (LBP) [1] is selected as baseline. The success of LBP in face description is due to the discriminative power, computational simplicity of the operator, and its robustness to monotonic gray scale changes caused by, for example, illumination variations. The use of histograms as features also makes the LBP approach robust to face misalignment and pose variations to some extent. For 2D FR, we use the operator $LBP^{u2}_{8,2}$ on 8×8 blocks. The similarity between each image pair is computed with chi-square distance metric. Performances are evaluated using the similarity scores between image pairs.

3.2.1. Evaluation on 2D and 3D Face Recognition

In this part, the evaluations are done for 2 modes. The first mode is the baseline mode: a standard biometric system with no spoofing and no countermeasure. The baseline performance is evaluated using DB-r. Performance is evaluated by verification all vs. all. Access from every identity in DB-r is tested against all other models in DB-r. The performance is measured by observing the rate of users rejected when authenticating against their own template (False Rejection Rate - FRR) and by the rate of users accepted when authenticating against someone else's template (False Acceptance Rate - FAR). The second mode is the evaluation of FR systems under mask attacks (baseline under attacks in Figure 3). Both DB-r and DB-m are used. When spoofing attacks are applied, performance is expected to degrade. In this mode, the FAR corresponds to the rate of attacks that are

accepted by the system when spoofed. The FRR corresponds to the rate of real-access attempts that are incorrectly dismissed by the system as attacks.

For the evaluations regarding 2D and 3D FR systems here, only test set is used. Train set is used for classifier training inside the proposed counter-measures. Figure 3 shows the behavior of the 3D and 2D baseline systems with/without attacks. All results are presented in terms of detection error trade-of (DET) profiles which illustrate the behavior of a system as the decision threshold is changed, i.e. how the false rejection rate varies according to the false acceptance rate.

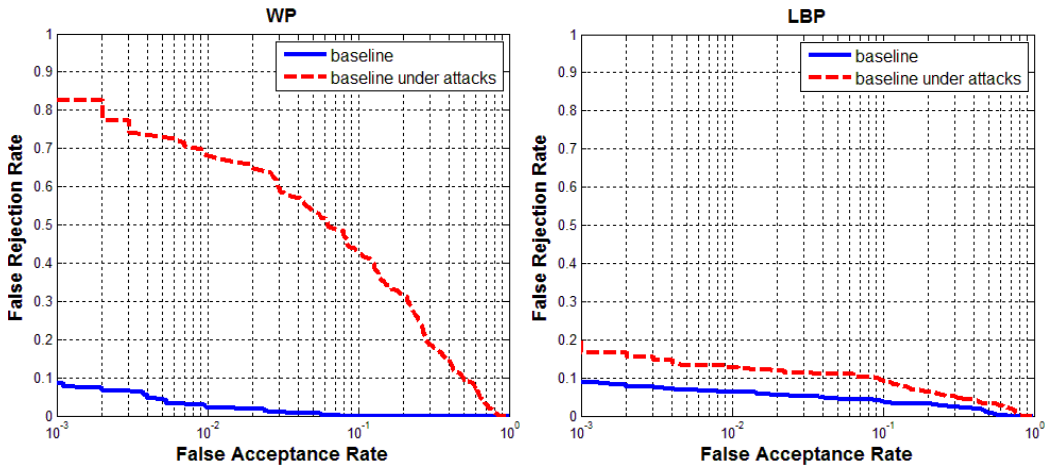


Figure 3: The DET Curves of the 3D and 2D face baseline biometric system with/without mask attacks, respectively.

Figure 3 shows that:

- Although the mask attacks are successful to spoof both 2D and 3D FR systems, the 3D FR system is more vulnerable to mask attacks compared to the 2D FR system (area between red and blue curves is

much more for 3D compared to 2D FR system).

- Equal Error Rate (EER) at the baseline mode increases from 1.8% to 25.1% for 3D and from 4.7% to 9.9% for 2D FR system under attacks.

- 3D shape characteristics of a real face and corresponding mask attack are more similar compared to their texture characteristics. Hence, analysis on texture may reveal more information to detect mask attacks compared to analysis on 3D shape characteristic.

- Robustness against mask spoofing is observed to be both method and modality dependent as also concluded in [16].

- FR systems are vulnerable to spoofing mask attacks hence, countermeasures are necessary to reduce their impact on face recognition.

For the baseline mode evaluations, we used the test set of DB-r, which contains 100 real samples from 10 subjects. In this study, we also report the baseline performances of the selected systems on the Face Recognition Grand Challenge Database (FRGC) v1.0 [25] database in order to check if the selected systems still provide satisfactory baseline performances with more number of subjects. The scans of the subjects in the mask database were acquired with a high quality laser scanner (technology of MORPHO). The FRGC database was also prepared using the high quality laser scanner Minolta. Therefore, the scan quality in the FRGC is quite similar to the scan quality in our mask database. Furthermore, FRGC v1.0 includes 943 samples

from 275 subjects and more challenging compared to the DB-r of the mask database. Table 1 shows the EER, verification rate at 0.001 FAR and rank-1 identification rates computed with the selected systems using both the mask database (the DB-r of the mask database) and the FRGC database.

Table 1: EER, Verification Rate at 0.001 FAR and Rank-1 Identification Rate (IR) for the 3D and 2D baseline systems using the Mask Database (MD) and the FRGC Database.

Techniques	**WP**		**LBP**	
	(MD)	(FRGC)	(MD)	(FRGC)
EER (%)	1.79	2.41	4.68	2.96
VR at 0.001 FAR (%)	91.33	87.70	90.89	90.03
IR (%)	100	94.01	98.89	94.50

Table 1 shows that slightly better performances are obtained in terms of identification and verification using the mask database compared to the ones obtained using the FRGC. For each FR technique, EER computed for the two databases are quite similar. Although there is a high increase in the number of subjects/samples when the FRGC is used for the evaluation, the performances of the selected baseline systems on the FRGC are still satisfactory, even quite similar to the results obtained using the mask database. These results show that the selected systems provide significant performances hence they are appropriate for this study, and the number of subjects/samples in the mask database is sufficient enough to obtain consistent results in this study.

4. TECHNIQUES USED INSIDE THE PROPOSED COUNTERMEASURES

Mask attack is a 3D attack that can be used to spoof both 2D and 3D FR systems. Most of the existing 3D scanners do not provide only 3D scan, they also capture texture image. Figure 1 shows an example for the two outputs of a scanner. Thus, when there is only one camera for 2D and one scanner for 3D FR system, a countermeasure which uses texture images as input can be used to protect both 2D and 3D FR systems if texture images are provided as default output of a scanner. In the present study, we propose four countermeasures against 3D mask attacks, which use either the depth maps or texture images as input (Figure 5).

In this section, we first explain the pre-processing applied for the proposed countermeasures. Then, we give a detailed information about the techniques that were used to develop the proposed countermeasures.

4.1. Pre-Processing for the Countermeasures

There are slight alignment differences between faces in the mask database. For the countermeasures, initially, all 3D faces in DB-r3 and DB-m3 are aligned to a generic face using LSS alignment, which makes the alignment of all faces identical.

In this study, we want to benefit from the information that the mask surface is smoother than the real face surface to detect mask attacks. Therefore, the depth maps are estimated from the raw aligned 3D scans. Next, 2D

cropping is applied to extract face region from both the texture images and depth maps. Then all images are resized into 64×64 grayscale image.

In our previous studies [15, 17], we used normalized images. We notice that normalization has a positive impact in performances when the countermeasure is applied on depth maps, whereas it reduces performances slightly when applied on texture images. In the present paper, we did not apply normalization, and we improved our cropping code compared to the ones used in our previous studies. The final version of the texture images and depth maps used for the proposed countermeasures are shown in the second and fourth columns of Figure 1, respectively.

4.2. The Variational Retinex Algorithm

In the present paper, the image is decomposed into reflectance and illumination components using the variational retinex algorithm explained in the studies [2, 12].

In this subsection, we first give information about minimizing energy functions. Then, we explain the variational retinex algorithm [2, 12].

4.2.1. Minimizing Energy Functions

The concept of minimizing the energy of a given system is used in image processing. Minimizing energy functions often includes solving partial differential equations, more specifically, Euler-Lagrange differential equations.

In the Euler-Lagrange problem, we usually have a continuous real-valued function $y = f(x)$ with continuous derivative $y\prime = df/dx$. Considering x, y,

and $y\prime$ as three independent variables, a new function $g(x, y, y\prime)$ is defined. Using this function, the energy function is defined as: $E = \int g(x, y, y\prime)dx$. The energy function E has a minimal value if Euler-Lagrange equation:

$$\frac{\partial g}{\partial y} - \frac{\partial}{\partial x}\left(\frac{\partial g}{\partial y\prime}\right) = 0 \tag{1}$$

is satisfied. The left hand side of this equation is denoted as ∇E. Here f is introduced as a function of one independent variable x, the same concept is applied when f is a function of n independent variables: $x1, x2, \ldots, xn$. In particular, when $u = f(x, y)$, function of two independent variables x and y, Euler- Lagrange equation becomes:

$$\nabla E = \frac{\partial g}{\partial u} - \frac{\partial}{\partial x}\left(\frac{\partial g}{\partial u_x}\right) - \frac{\partial}{\partial y}\left(\frac{\partial g}{\partial u_y}\right) = 0 \tag{2}$$

The variational retinex algorithm is developed by defining and minimizing an energy function.

4.2.2. The Variational Retinex Algorithm

An image can be considered as a two dimensional function $S(x, y)$, where (x, y) denotes a pixel on the image. The value of the function $S = S(x, y)$ represents the intensity of the light at the pixel (x, y). As stated in [2], the intensity S may be characterized by two components which are;

- the amount of source illumination falling on the object, the illumination component $L(x, y)$.

- the amount of illumination reflected by the object, the reflectance component $R(x, y)$.

$S(x, y)$ is computed using the illumination and reflectance components as shown in Eq. (3).

$$S(x, y) = L(x, y) \times R(x, y) \tag{3}$$

In [2], it is stated that if images are assumed to be composed of illumination and reflectance components, generating the retinex effect means being able to separate one component from another. A first step taken by most algorithms in such sort of problems is the conversion to the logarithmic domain by $s = log(S)$, $l = log(L)$, and $r = log(R)$. In the logarithmic domain the relation between these three images becomes: $s = l + r$.

In [12], Kimmel et al. make the following assumptions:

1. The logarithmic illumination l varies spatially smoothly.
2. The logarithmic reflectance r consists of constant or smooth parts and discontinuous jump parts.
3. l is greater than or equal to the logarithmic intensity s ($l \geq s$).
4. l is close to s (i.e. l does not deviate far away from s).

Based on the assumptions listed above, in the studies [2, 12], the energy function is defined as follows:

$$E(l) = \int (|\nabla l|^2 + \alpha(l - s)^2 + \beta|\nabla(l - s)|^2)dxdy \tag{4}$$

where α and β are positive constants. Since S is the given image, s here is constant. In this equation;

- The first penalty term ($|\nabla l|^2$) forces spatial smoothness on l.
- The second penalty term $(l-s)^2$ forces a proximity between l and s. The difference between these images is exactly r, which means that the norm of r should be small. Simultaneously, it forces the solution l to be $l \geq s$. In [12], it is stated that in practice this term should be weak enough not to attract l down too much towards s. This is why the parameter α should be very small.
- The third term forces r to be spatially smooth. In [12], it is stated that the parameter β should be a very small value to preserve the discontinuous jumps of r. Note that spatially smooth r contradicts spatially smooth l since $r + l = s$. However in practice adding this penalty term kicks in mainly on sharp edges and handles situations where the illumination is not smooth (as well as cases of direct light sources and specularities).

The integrand of this energy function is:

$$\begin{aligned} g(l, l_x, l_y) &= |\nabla l|^2 + \alpha(l-s)^2 + \beta|\nabla(l-s)|^2 \\ &= (l_x^2 + l_y^2) + \alpha(l-s)^2 + \beta((l_x - s_x)^2 + (l_y - s_y)^2) \end{aligned} \tag{5}$$

Euler-Lagrange equation becomes:

$$\begin{aligned}\nabla E &= \frac{\partial g}{\partial l} - \frac{\partial}{\partial x}\left(\frac{\partial g}{\partial l_x}\right) - \frac{\partial g}{\partial y}\left(\frac{\partial g}{\partial l_y}\right) \\ &= 2\alpha(l-s) - \frac{\partial}{\partial x}\left(2l_x + 2\beta(l_x - s_x)\right) - \frac{\partial}{\partial y}\left(2l_y + 2\beta(l_y - s_y)\right) \\ &= 2\alpha(l-s) - 2l_{xx} - 2\beta(l_{xx} - s_{xx}) - 2l_{yy} - 2\beta(l_{yy} - s_{yy}) \\ &= 2\left[\alpha(l-s) - \Delta l - \beta\Delta(l-s)\right] \\ &= 0\end{aligned} \tag{6}$$

which means $\alpha(l-s) - \Delta l - \beta\Delta(l-s) = 0$. In [2], to solve this equation, the idea of the steepest descent is applied with an auxiliary variable t:

$$\frac{dl}{dt} = -\nabla E = \Delta l + \beta\Delta(l-s) - \alpha(l-s) \tag{7}$$

To find a local minimum of a function using steepest descent, one takes steps proportional to the negative of the gradient of the function at the current point. In our evaluation, l is computed via steepest descent as follows:

$$l_n = l_{n-1} - dt \cdot \nabla E \tag{8}$$

Finally, projecting onto the constraint $l \geq s$ is done by $l_n = max(l_n, s)$.

In our experiments, the values 0.0001 and 0.1 are used for α and β, respectively, as suggested in [2, 12]. The initial value of l (l_0) is taken as s. The step size dt and the total number of iterations are selected as 0.05 and 5000, respectively. After the iterations, optimum l is obtained, and

r is computed from $r = s - l$. Finally, the reflectance and illumination components are evaluated from $R = e^r$ and $L = e^l$, respectively.

Figure 4: Example from the mask database which is created by [23] (a) The real face with texture, the reflectance image and the illumination image of the real face (b) Same images associated with the mask of the same person.

Figure 4 shows an example from the mask database for a real face and corresponding mask attack. First column shows the original images, second column and third column show the reflectance and illumination images, respectively, which are computed using the variational retinex algorithm.

4.3. Micro-Texture Analysis Technique

The micro-texture analysis, which was first proposed in [20] to detect 2D face attacks, is used to detect 3D mask attacks here. In [20], it is applied on texture images, whereas in this paper, we apply this technique not only on texture images but also on depth maps estimated from 3D scans and on reflectance components of texture images.

This LBP based micro-texture analysis technique emphasizes the micro-texture differences in the feature space. It aims at learning the differences between real and fake face, and designs a feature space which emphasizes those differences. The original LBP forms labels for the image pixels by thresholding the 3×3 neighborhood of each pixel with the center value and considering the result as a binary number. The LBP operator has been extended to use neighborhoods of different sizes. $LBP_{P,R}$ is computed such that for a given central pixel in an image, a pattern number is computed by comparing its value with those of its neighbors. In Eq. (9), g_c is the gray value of the central pixel, g_p is the value of its neighbors, P is the number of neighbors around a circle of radius R. $LBP_{P,R}$ calculation is shown in Eq. (9) and (10):

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p \tag{9}$$

$$s(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x<0 \end{cases} \tag{10}$$

Uniform patterns are verified to be the fundamental patterns of local image texture. A local binary pattern is called uniform if the binary pattern contains at most two bitwise transitions from 0 to 1 or vice versa when the bit pattern is traversed circularly. The notation is $LBP^{u2}_{P,R}$. $u2$ stands for using only uniform patterns and labeling all remaining patterns with a single

label.

In [20], authors claim that micro-texture details that are needed to discriminate a real face from face print can best be detected using combination of different LBP operators. Thus, they derive an enhanced facial representation using multi-scale LBP operators. Their proposed representation computes LBP features from 3×3 overlapping regions to capture the spatial information and enhances the holistic description by including global LBP histograms computed over the whole image. This is done as follows: the face is cropped and resized into a 64×64 pixel image. Then, $LBP^{u2}_{8,1}$ operator is applied on the face image and the resulting LBP image is divided into 3×3 overlapping regions (with an overlapping size of 14 pixels). The local 59-bin histograms from each region are computed and collected into a single 531-bin histogram. Then, two other histograms are computed from the whole face image using $LBP^{u2}_{8,2}$ and $LBP^{u2}_{16,2}$ operators, yielding 59-bin and 243-bin histograms that are added to the 531-bin histogram previously computed. In [20], the length of the final enhanced feature histogram is reported as 833 (i.e. $531 + 59 + 243$).

4.4. Classification Technique

Mask face detection is a two-class classification problem. Since SVM [8] are proven to be a powerful tool for discriminating two classes of data, we adopted an SVM classifier for this purpose. SVM finds the maximum margin hyper-plane to separate the training data in feature space and a decision for

a new test data x is classified. In our experiments, we adopted linear kernel since our feature vectors are high-dimensional and are hence likely to be linear separable.

5. THE PROPOSED COUNTERMEASURES

Four countermeasures are proposed in this study to discriminate mask and real samples. Three of them use the 2D data (texture images), and the remaining one uses the 3D data (depth maps estimated from the raw 3D scans) available in the mask database as input.

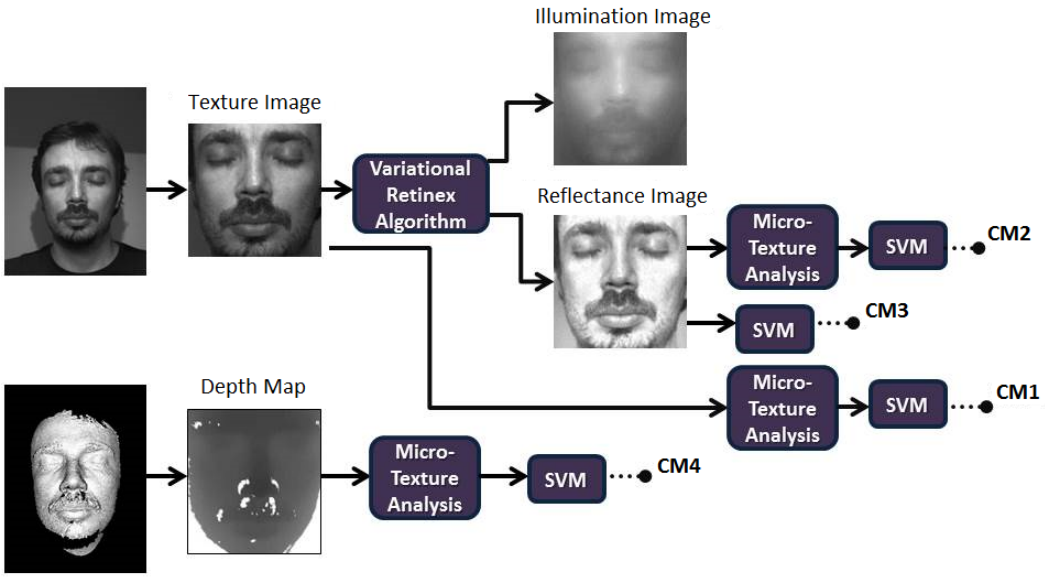


Figure 5: The flowchart of the proposed countermeasures.

The flowchart of the countermeasures proposed in this paper are shown in Figure 5. In this figure, the micro-texture analysis (explained in Subsection 4.3) applied on texture images is called CM1, applied on reflectance images

is called CM2, applied on depth maps is called CM4, and finally the countermeasure for which the pixel intensity values on reflectance images are used directly by the classifier is called CM3 (CM denotes countermeasure).

CM1 and CM4 are first introduced in our study [15], and CM3 is first introduced in our study [17]. In the present paper, we provide an overview on our spoofing detection approaches introduced in the studies [15, 17]. We extend the works explained in these studies with some improvements (e.g. better cropping, usage of non-normalized images instead of normalized images), additional analysis, comparisons of performances of diverse countermeasures using the same protocol, and with a detailed analysis of the fusion scenarios. Also, CM2 is first introduced in the present paper. It is a new countermeasure providing very satisfactory accuracy to classify mask and real faces. The results of CM2 show that reflectance component of an image provides more appropriate information than original image itself for mask detection. From the fusion results, we also observed that it provides complementary information on mask detection.

5.1. CM1: Micro-Texture Analysis on Texture Images

Captured image from mask may visually look very similar to the image captured from live face (e.g. the texture images in the first column of Figure 4). A close look at the differences between faces in DB-r2 and DB-m2 reveals that their surface properties are different. For mask manufacturing 3D printers are used, hence they may contain printing quality defects that

can be detected with micro-texture patterns. For CM1, micro-texture analysis is applied on texture images, and the feature histogram of length 833 is obtained. Finally, linear SVM classifier is applied to detect mask and real faces.

5.2. CM2: Micro-Texture Analysis on Reflectance Images

For CM2, initially, the illumination and reflectance components (Figure 5) of the texture images are obtained using the variational retinex algorithm introduced in Subsection 4.2. Then, micro-texture analysis is applied on reflectance components of texture images rather than texture images itself. The reason of this analysis on reflectance images is that a close look at the differences between the reflectance images of the real and mask faces reveals that the texture characteristics on their reflectance components are also different. The feature vectors of length 833, which are obtained by applying micro-texture analysis on reflectance images, are used as input by linear SVM classifier. This feature vector gives information from the reflectance image in the image texture level.

5.3. CM3: Pixel Intensity Analysis on Reflectance Images

Our observations on the reflectance components of mask and real faces reveal that reflectance characteristics of mask and real face samples are different especially at some specific regions of the face (eyelashes, eyebrows and moustache). Based on these observations, in this study, we use the intensity

values on reflectance component of each image as input for linear SVM classifier. Since the intensity values on reflectance images are between 0 and 1 ($R(x, y) \in [0, 1]$), we stretched it to the interval [0, 255] by multiplying R with 255. The reflectance component, which is in the size of 64×64 pixel image, is reshaped as [1 4096] ($64 \times 64 = 4096$). The resultant vector is the feature vector providing information in the pixel intensity level. Finally, linear SVM classifier is applied to detect real and mask faces.

5.4. CM4: Micro-Texture Analysis on Depth Maps

The 3D shape of high quality mask is also very similar to the 3D shape of corresponding real face (e.g. the 3D scans in the second column of Figure 1). Our analysis on DB-r3 and DB-m3 show that the mask scan is smoother than the real face scan. Especially the parts of the face with facial hair are quite different. Since there is no real facial hair (e.g. mustache, eyebrow) on the masks, the 3D scan of mask is smoother in these parts compared to the real face scan. When high quality scanners are used for acquisition, although there is a decrease in the number of holes, it is still possible to observe some holes on the scan especially at the parts of the face with facial hair. Thus, in our study, micro-texture analysis is also applied on the depth maps which are estimated from the raw 3D scans, and the other feature histogram of length 833 is obtained. Finally, linear SVM classifier is applied to detect real and mask faces.

6. EXPERIMENTS AND RESULTS

In this section, we first show the stand-alone classification performances of the proposed countermeasures together with the fusion scenarios. Then, we integrate the countermeasure providing the best performance to the selected 3D FR system in order to observe the improvement in the recognition performance of the system in presence of mask attacks.

6.1. Stand-Alone Classification Performances of the Countermeasures

In the present study, we apply the proposed countermeasures (CM1, CM2, CM3, CM4) using the same database with the same train-test sets, hence an exact comparison between these countermeasures is possible. Train set is used for classifier training. This classifier is subject to two kind of errors:

- FLR (False Living Rate), that represents the percentage of fake data misclassified as real. (similar to FAR)
- FFR (False Fake Rate), which computes the percentage of real data assigned to the fake class. (similar to FRR)

The lower these two errors, the better the performance of the countermeasures. In this section, we first evaluate the performances of the single countermeasures, and then evaluate the performances for the fusion scenarios. The Region of Convergence (ROC) curves in Figure 6 shows the stand-alone classification performances of the four countermeasures together with the fusion based countermeasure providing the best performance in Table 3.

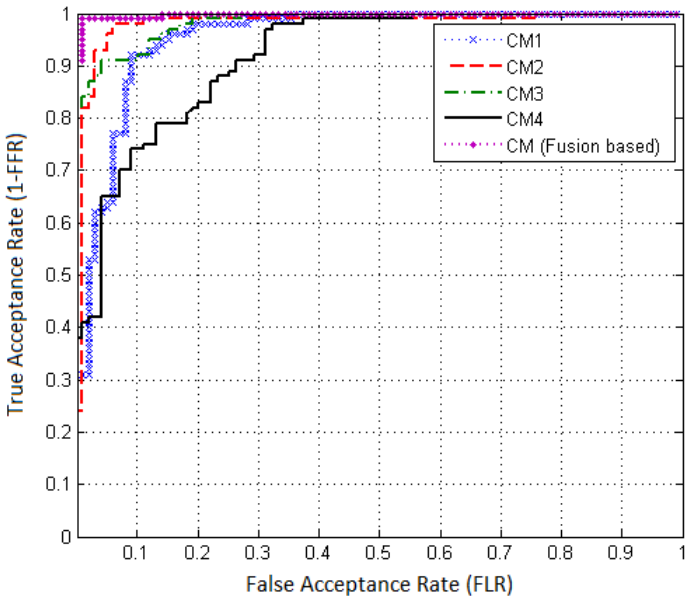


Figure 6: The Classification Performances of the Countermeasures.

Area Under Curve (AUC), EER and best accuracy results using CM1, CM2, CM3, and CM4 are shown in Table 2.

Table 2: AUC, EER and Accuracy Results Using the Four Countermeasures

Countermeasures	**AUC**	**EER(%)**	**Accuracy(%)**
CM1	0.956	9.04	91.46
CM2	0.980	**5.02**	**95.98**
CM3	**0.984**	9.04	93.47
CM4	0.919	18.59	82.91

Table 2 and Figure 6 show that;

- The best performances in terms of EER and accuracy are obtained using CM2, and the best performance in terms of AUC is obtained using CM3.

- The best performances are obtained with the countermeasures based on reflectance analysis (CM2 and CM3) compared to the performances obtained with CM1 and CM4. This shows that reflectance characteristics of the real and mask faces in the mask database provide more appropriate information than their texture and smoothness characteristics.

- CM4, which is based on smoothness analysis, provides worse results compared to the other countermeasures. However, the performance of CM4 can be still considered as satisfactory.

- 2D data (texture images) provide more information than 3D data (depth maps) to detect mask spoofing.

After evaluating the performances of the single countermeasures, we analyze the performances for the fusion scenarios.

For feature level fusion, the feature histograms computed from different types of images (texture, reflectance and depth) are concatenated and the classifier is applied on the resultant feature histogram. In Table 3, the feature level fusion of 2 countermeasures, 3 countermeasures and finally all the 4 countermeasures are reported for which the length of the final feature histograms are 1666, 2499 and 3332, respectively. Once the enhanced histogram is computed, a linear SVM classifier is used to determine whether the image corresponds to a live face or not.

For score level fusion, linear SVM classifier is applied using the features computed from each type of images (texture, reflectance and depth) separately, and then Z-score normalization is applied for each score group. Finally, the weighted score level fusion is used for combining the outputs of the individual SVMs to determine whether the image corresponds to a live face or not.

AUC, EER and best accuracy results are shown in Table 3 for the fusion scenarios.

Table 3: AUC, EER and Accuracy Results for the Fusion Scenarios of the Proposed Countermeasures

Countermeasures Involved in Fusion	**Feature Level Fusion**			**Score Level Fusion**		
	AUC	**EER (%)**	**Acc. (%)**	**AUC**	**EER (%)**	**Acc. (%)**
CM1, CM2	0.994	3.01	97.49	0.988	3.01	97.49
CM1, CM3	0.985	9.04	93.97	0.993	5.02	96.48
CM1, CM4	0.972	9.04	92.96	0.976	8.04	94.47
CM2, CM3	0.984	9.04	93.47	0.993	5.02	96.48
CM2, CM4	0.994	3.01	97.49	0.992	4.02	96.98
CM3, CM4	0.986	8.04	92.96	0.994	5.02	95.98
CM1, CM2, CM3	0.985	9.04	93.47	**0.998**	**2.01**	**98.99**
CM1, CM2, CM4	**0.998**	**2.01**	**97.99**	0.993	5.02	96.48
CM1, CM3, CM4	0.987	8.04	93.47	0.997	2.01	97.99
CM2, CM3, CM4	0.986	8.04	93.47	0.997	2.00	98.49
CM1, CM2, CM3, CM4	0.987	8.04	93.47	0.997	2.01	98.49

From the reported results in Table 3, we can remark the followings:

- Both score and feature level fusion of the countermeasures improve the performance compared to using single countermeasure. For instance, CM4 provides a detection accuracy of 82.9% whereas when CM4 and

CM1 are fused, the accuracy is improved to 92.96% for feature and 94.47% for score level fusion. This proves that when both the texture images and depth maps are provided by 3D scanners, more robust countermeasures can be obtained by fusion.

- For feature level fusion, the best performances are obtained by the fusion of CM1, CM2 and CM4. In this part, we observed that when we concatenate the same type of features (micro-texture features of length 833 for each of CM1, CM2 and CM4), we observe a significant increase in the performance. In CM3, the features are pixel intensity values (features of length 4096). Therefore, when we apply feature level fusion using CM3 with the other countermeasures, the positive impact of CM3 in the performances was not observable as shown in Table 3.

- For score level fusion, the best performances are obtained by the fusion of CM1, CM2 and CM3. All these countermeasures (CM1, CM2 and CM3) uses texture images as input (reflectance image is computed from texture image). This proves that 2D data provides very beneficial information for mask spoofing detection.

- CM3 increases the performances when it is used in score level fusion, whereas the impact of it in feature level fusion is not remarkable.

- Although CM1, CM2 and CM3 provide very satisfactory results alone, the score level fusion of these countermeasures provides the best performance compared to all other scenarios in Table 2 and 3. Therefore, in

Figure 6, the ROC curve of this fusion based countermeasure is shown as the best one.

- Since existing 3D scanners provide both 3D scan and corresponding texture image, more robust countermeasures can be developed by fusion of these two type of outputs (2D and 3D data).

6.2. Integration of the Countermeasure to Face Recognition Systems

In this subsection, we integrate the countermeasure with the best performance (fusion of CM1, CM2 and CM3) to the 3D FR system selected as baseline.

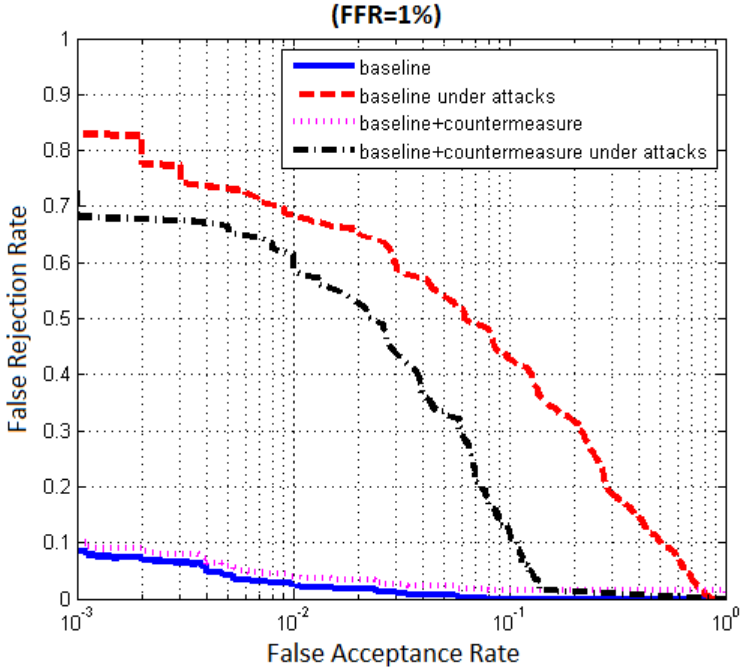
The evaluations are done for 4 modes. The first two modes are the baseline mode and the mode under attacks, which are explained in Subsection 3.3. The third mode illustrates performance when the countermeasure is applied against the attacks, that results in an improved performance with respect to the second mode. For the samples which are detected as attack by the countermeasure, a least similarity score, which is zero in this test, is assigned to those samples in verification tests. Last mode evaluates the performance of the baseline system together with the countermeasure in the normal operation mode of system, i.e., without attacks. The inclusion of the countermeasure may degrade the baseline performance when not confronted to attack (e.g. the countermeasure may consider as fake some real users.).

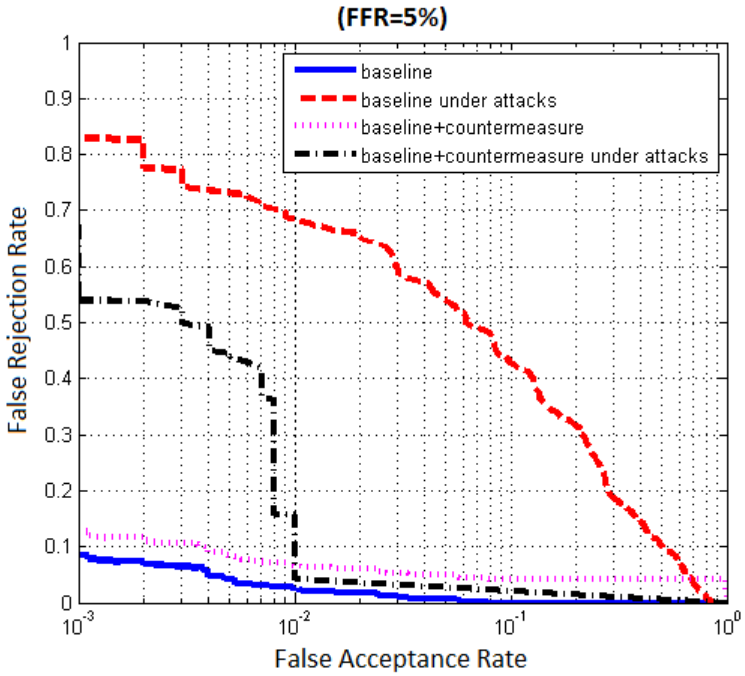
For evaluations, we fix 3 different evaluation points at FFR = 1%, 5%, and 10% (FFR and FLR were defined in the previous subsection). Once

fixed, we incorporate the countermeasure as a first step into the baseline biometric systems oriented to discard fake data, and generate the performance evaluations for the 4 modes explained above.

Figure 7 shows the behavior of the 3D face baseline system with/without attacks and with/without the countermeasure. The three figures represent the overall system performance under spoofing attacks when three different operating points (FFR = 1%, 5%, and 10%) are used for adjusting the countermeasure.

It is clear from Figure 7 that the 3D FR system is vulnerable to mask attacks (more area between blue and red curves indicates more vulnerability to the attacks). Performance enhancement is obtained almost all regions of DET plots in Figure 7 when the countermeasure is introduced in presence of mask attacks (black curve compared to red curve). If we take an operating point where FFR = 1%, then FRR of the 3D FR system under attacks drops from around 65% to around 50% at FAR = 2%. For both of the two other plots (at FFR = 5% and 10%), the introduction of the countermeasure lowers FRR from around 65% to 4% and 7%, respectively, at FAR = 2%. The performance of the countermeasure is observed to be better at FFR = 5% compared to the cases at FFR = 1% and 10%. Finally, the inclusion of the countermeasure improves the results of 3D FR system under attacks, whereas it degrades baseline performances of the system when not confronted to attack (pink curve compared to blue curve).


(FFR=1%)
baseline
baseline under attacks
baseline+countermeasure
baseline+countermeasure under attacks
False Rejection Rate
False Acceptance Rate
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
10^-3
10^-2
10^-1
10^0


(FFR=5%)
baseline
baseline under attacks
baseline+countermeasure
baseline+countermeasure under attacks
False Rejection Rate
False Acceptance Rate
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
10^-3
10^-2
10^-1
10^0

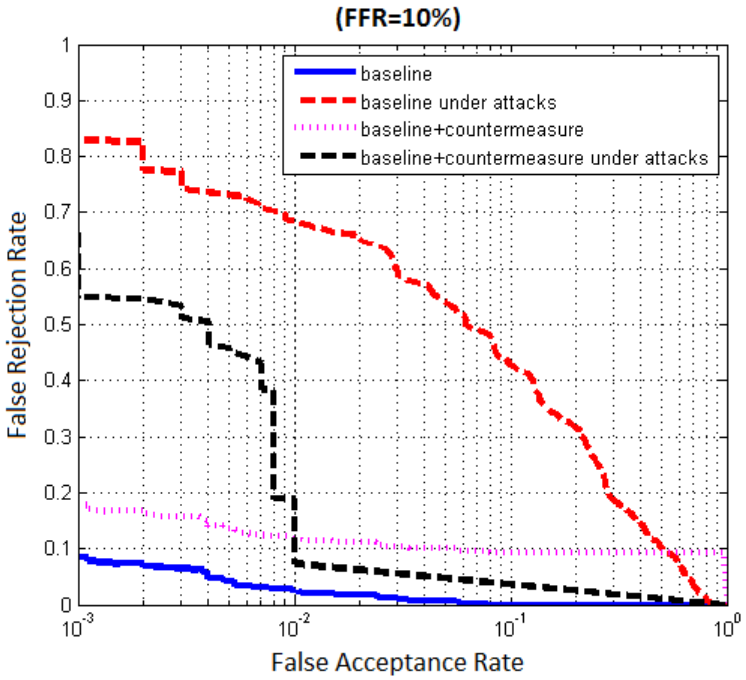


Figure 7: The DET Curves of the 3D face baseline biometric system when integrating the countermeasure.

7. CONCLUSIONS

In this study, a 2D+3D mask attack database is used to evaluate the performances of the proposed countermeasures for the protection of face recognition systems against mask attacks.

The novelty of this study is that it is still one of the few studies that proposes countermeasures against 3D mask attacks. The analysis are done on depth maps, texture images and reflectance components of texture images, and 4 different countermeasures are proposed. Three of the proposed countermeasures use 2D data (texture images), and the remaining one uses 3D data (depth images) as input. These countermeasures can be used to protect

both 2D and 3D FR systems against mask attacks. The results of this study show that analysis on reflectance images provide the best results compared to analysis on texture and depth images. All of the 4 countermeasures provide satisfactory information hence can be used as independent sources to discriminate masks from real faces. However with the fusion of these countermeasures, we observe a significant improvement in the performances. For instance, in this paper, a classification accuracy of 99% (almost perfect accuracy) is achieved for real face vs. mask face by fusing the information extracted from the reflectance images and texture images.

Up to now, we have analyzed several characteristics of real and mask faces, and obtained almost perfect results on this mask database. The limitation of our study is that we were able to test the performances of the proposed countermeasures using the masks made from one type of material, which is polychrome mineral powder. When masks made from different materials are used, we may obtain different performance accuracy. Our future works are first to test the performances of the proposed countermeasures using masks made from different materials in order to observe if we can still obtain satisfactory results, and then to propose new countermeasures for more challenging mask databases with higher number of subjects as soon as available.

Acknowledgment: This work has been performed by the TABULA RASA project 7th Framework Research Programme of the European Union (EU), grant agreement number: 257289. The authors would like to thank

the EU for the financial support and the partners within the consortium for a fruitful collaboration. For more information about the TABULA RASA consortium please visit http://www.tabularasa-euproject.org.

References

[1] T. Ahonen, A. Hadid, M. Pietikainen, Face description with local binary patterns: Application to face recognition, IEEE Trans. on Pattern Analysis and Machine Intelligence (2006) 2037–2041.

[2] N. Almoussa, Variational retinex and shadow removal, Technical Report, The Mathematics Department, UCLA (2008).

[3] J. Bai, T.T. Ng, X. Gao, Y.Q. Shi, Is physics-based liveness detection truly possible with a single image?, IEEE International Symposium on Circuits and Systems (2010) 3425–3428.

[4] W. Bao, H. Li, N. Li, et al., A liveness detection method for face recognition based on optical flow field, Int. Conf. on Image Analysis and Signal Processing (IASP) (2009) 233–236.

[5] P. Besl, N. McKay, A method for registration of 3-d shapes, IEEE Trans. on Pattern Analysis and Machine Intelligence (1992) 239–256.

[6] F.L. Bookstein, Principal warps: Thin-plate splines and decomposition of deformations, IEEE Trans. Pattern Analysis and Machine Intelligence (1989) 567–585.

[7] M.M. Chakka, A. Anjos, S. Marcel, et al., Competition on counter measures to 2-d facial spoofing attacks, IEEE IAPR Int. Joint Conference on Biometrics (IJCB) (2011) 1–6.

[8] C.C. Chang, C.J. Lin, Libsvm : a library for support vector machines, ACM Transactions on Intelligent Systems and Technology (2011) 2:27:1–27:27.

[9] G. Chetty, M. Wagner, Multi-level liveness verification for face-voice biometric authentication, Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference (2006) 1–6.

[10] N. Erdogmus, J.L. Dugelay, On discriminative properties of tps warping parameters for 3d face recognition, IEEE Int. Conf. on Informatics, Electronics and Vision (ICIEV) (2012) 225–230.

[11] Y. Kim, J. Na, S. Yoon, J. Yi, Masked fake face detection using radiance measurements, Journal of the Optical Society of America A (2009) 760–766.

[12] R. Kimmel, M. Elad, D. Shaked, R. Keshet, I. Sobel, A variational framework for retinex, International Journal of Computer Vision (2003) 7–23.

[13] K. Kollreider, H. Fronthaler, J. Bigun, Verifying liveness by multiple experts in face biometrics, IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (2008) 1–6.

[14] N. Kose, J.L. Dugelay, Classification of captured and recaptured images to detect photograph spoofing, IEEE Int. Conf. on Informatics, Electronics and Vision (ICIEV) (2012) 1027–1032.

[15] N. Kose, J.L. Dugelay, Countermeasure for the protection of face recognition systems against mask attacks, IEEE Automatic Face and Gesture Recognition (FG) (2013) 1–6.

[16] N. Kose, J.L. Dugelay, On the vulnerability of face recognition systems to spoofing mask attacks, IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP) (2013) 2357–2361.

[17] N. Kose, J.L. Dugelay, Reflectance analysis based countermeasure technique to detect face mask attacks, Int. Conf. on Digital Signal Processing (DSP) (2013) 1–6.

[18] N. Kose, J.L. Dugelay, Shape and texture based countermeasure to protect face recognition systems against mask attacks, IEEE Computer Vision and Pattern Recognition Workshop, on Biometrics (CVPRW) (2013) 111–116.

[19] J. Li, Y. Wang, T. Tan, et al., Live face detection based on the analysis of fourier spectra, Proceedings of the SPIE (2004) 296–303.

[20] J. Maatta, A. Hadid, M. Pietikainen, Face spoofing detection from single images using micro-texture analysis, Proc. of IEEE Int. Joint Conf. on Biometrics (IJCB) (2011) 1–7.

[21] J. Maatta, A. Hadid, M. Pietikainen, Face spoofing detection from single images using texture and local shape analysis, IET Biometrics (2012) 3–10.

[22] M.D. Marsico, M. Nappi, D. Riccio, J.L. Dugelay, Moving face spoofing detection via 3d projective invariants, IAPR Int. Conf. on Biometrics (2012) 73–78.

[23] MORPHO, http://www.morpho.com/, 2010.

[24] G. Pan, L. Sun, Z. Wu, S. Lao, Eyeblink-based antispoofing in face recognition from a generic webcamera, IEEE Int. Conf. on Computer Vision (ICCV) (2007) 1–8.

[25] P.J. Phillips, P.J. Flynn, T. Scruggs, K. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, W. Worek, Overview of the face recognition grand challenge, IEEE Computer Society Conf. on Computer Vision and Pattern Recognition (2005) 947–954.

[26] PRINT-ATTACK Database, http://www.idiap.ch/dataset/printattack, 2010.

[27] Sculpteo 3D Printing, http://www.sculpteo.com/en/, 2009.

[28] TABULA RASA Project, http://www.tabularasa-euproject.org/, 2010.

[29] Z. Zhang, D. Yi, et.al, Face liveness detection by learning multispectral

772 reflectance distributions, IEEE Automatic Face and Gesture Recogni-
773 tion (FG) (2011) 436–441.