Reflectance Analysis Based Countermeasure Technique to Detect Face Mask Attacks

Neslihan Kose, Jean-Luc Dugelay
Multimedia Department
EURECOM
Sophia-Antipolis, France
{neslihan.kose, jean-luc.dugelay}@eurecom.fr

***Abstract*—Face photographs, videos or masks can be used to spoof face recognition systems. Recent studies show that face recognition systems are vulnerable to these attacks. In this paper, a countermeasure technique, which analyzes the reflectance characteristics of masks and real faces, is proposed to detect mask attacks. There are limited studies on countermeasures against mask attacks. The reason for this delay is mainly due to the unavailability of public mask attack databases. In this study, a 2D+3D face mask attack database is used which is prepared for a research project in which the authors are all involved. The performance of the countermeasure is evaluated using the texture images which were captured during the acquisition of 3D scans. The results of the proposed countermeasure outperform the results of existing techniques, achieving a classification accuracy of 94.47%. In this paper, it is also proved that reflectance analysis may provide more information for the purpose of mask spoofing detection compared to texture analysis.**

Keywords—face spoofing; mask attacks; countermeasure

I. Introduction

In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain access to the system. The observations show that face recognition (FR) systems are vulnerable to spoofing attacks, hence researchers started to work on countermeasures to reduce the impact of attacks on FR performances. Recently, there have been several studies on countermeasures to detect photograph and video attacks, which are 2D face attacks [1 - 3]. However, there are limited studies to detect 3D mask attacks. To the best of our knowledge, only in [4, 5], countermeasures are proposed to protect FR systems against mask attacks. The main reason for the lack of studies on mask spoofing is due to the unavailability of public mask databases. For this study, the mask database which is prepared within the context of a European Union (EU) research project TABULA RASA [6] is used.

Photograph and video attacks are 2D face attacks whereas mask attack is a 3D face attack. Camera is used for 2D FR systems to capture the image of a person and scanner is used for 3D FR systems to obtain the 3D scan of a person. Since camera captures the image of a mask attack (2D face image), we can say that mask attacks can be used to spoof both 2D and 3D FR systems. Furthermore, most of the existing 3D scanners do not provide only 3D scan, they also capture texture image. Fig. 1 (a) & (b) shows an example for the two outputs of a scanner. Therefore, in case of no additional hardware (only one camera for 2D FR system and one scanner for 3D FR system), a countermeasure which is developed by using only texture images can be used to protect not only 2D but also 3D FR systems if the texture images are provided as default output of the scanner.

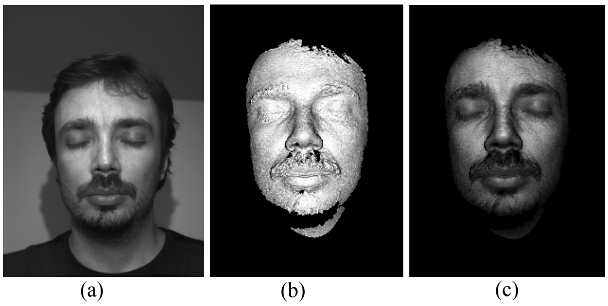
(a) (b) (c)

Figure 1. Example from the mask attacks database created by [7] (a) Texture image (the default output of most existing 3D scanners) (b) the snapshot of 3D scan (the default output of 3D scanners) (c) the snapshot of the 3D scan with texture that is obtained when the texture image (a) is mapped on the scan (b).

To the best of our knowledge, there are only a few studies to detect mask attacks [4, 5]. In [4], they present a multispectral face liveness detection method. They analyze the problem based on the Lambertian reflectance model, followed by the multispectral light selection and classification process to detect mask attacks. Mask faces are less common and more difficult to detect compared to planar faces. The reasons are: firstly, masks are 3D objects hence they are more like a genuine face than a 2D planar face and secondly, the materials of masks, such as silica gel and rubber, is more closer to human skins in reflectance than paper-based photos and glass-based video screens [4]. In the study of Zhang et al. [4], 20 masks are used, each sampled 5 times and 40 person are used each sampled 3 times (120 positive and 100 negative samples). They achieved 89.18% mean detection accuracy of real face vs. mask face. In our previous study [5], we propose a texture analysis based countermeasure technique to detect mask spoofing. The mask attack database which is used in our previous study [5] and also in this study was created by MORPHO [7]. The details of this mask database are explained in the next section. Since this mask database includes many high quality samples, it provides significant advantage to evaluate the performances of the countermeasures to detect mask attacks. In the present study, the countermeasure in [5] is also applied using the same database with the same test-training partitioning in order to make an exact comparison with the proposed countermeasure.

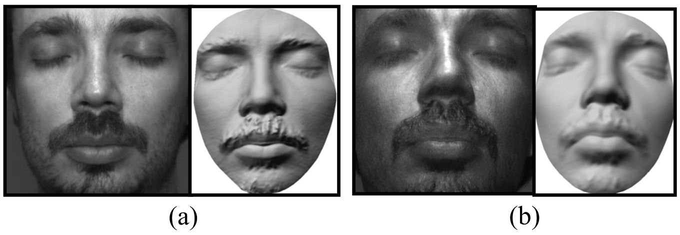

Figure 2. Example from the mask database which is created by [7] (a) The real face with texture and without texture after preprocessing (filling holes, removing spikes, smoothing and cropping) (b) The mask of the same person with texture and without texture after preprocessing.

In [5], we analyze the texture characteristics of masks and real faces, whereas in this study, we analyze the reflectance characteristics of masks and real faces to detect mask spoofing. The countermeasure in [5] is applied on both the texture images (the default outputs of the scanner used by [7] while creating the mask database, e.g. texture images in Fig. 2) and the range images, separately, whereas in the present study, the proposed countermeasure is a reflectance analysis based technique, this is why it is applied only on the texture images to detect mask spoofing.

The proposed countermeasure does not need any extra hardware and user collaboration. The technique relies on a single image and is easy to implement.

The novelties of our study can be listed as follows:

- The proposed countermeasure technique is based on reflectance analysis to detect mask attacks. This study is one of the few countermeasure studies against mask attacks and is advantageous in terms of the computational cost, and in terms of performances compared to the other studies [4, 5].
- Existing 3D scanners provide also texture images. In this study we apply the countermeasure on the texture images. Therefore, in case the proposed countermeasure is successful on texture images, it can be used to protect both 2D and 3D FR systems against mask attacks.
- The performance of the countermeasure is compared with the performance of an existing countermeasure [5] in this paper. Both techniques use the same mask database with the same test-training partitioning hence a comparison between the countermeasures is possible.
- In [5], it is proved that the texture characteristics of masks and real faces are different. In this paper, it is proved that their reflectance characteristics is also different, thus reflectance analysis provides satisfactory results as a countermeasure to protect FR systems against mask attacks.

The paper is organized as follows: Section II gives brief information on the mask database which is used in this study. Section III explains the proposed countermeasure technique. Section IV shows the experiments and results. Finally, conclusions are provided in Section V.

II. The Mask Database

A mask is an object normally worn on the face, typically for protection, performance or entertainment. In this study, the impact of mask attacks that are used for spoofing purposes is analyzed.

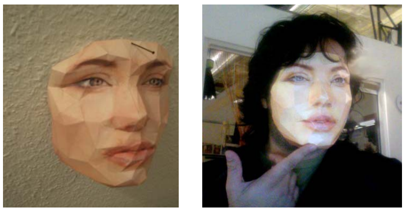

Figure 3. Example sample for paper mask. In the second column, the mask in the first column is worn on the face. The picture is taken from [8].

There are several ways of mask manufacturing. A mask of a person can be prepared even by using papers (Fig. 3). The mask which is used for 3D face spoofing purposes needs to show very similar 3D face shape characteristics of the target face to be considered as a successful attack. The mask database used in this study was prepared according to this purpose. To obtain similar face shape characteristics of the target person, initially, the scans of the subjects in the mask database were taken by a 3D scanner which uses a structured light technology. Then the 3D mesh was obtained for each subject, which is the projection of the acquisition into a 3D model. In the final step, each 3D model was sent to the 3D printer and masks were manufactured by Sculpteo 3D Printing [9].

In the mask database, 20 subjects appear in total. The masks are manufactured for only 16 of these subjects. In this database, these 16 subjects appear with both their own mask and also with masks of other people. The remaining 4 subjects appear with masks of the other 16 subjects. For each subject, average 10 scans are taken for the original person (real accesses) and average 10 scans are taken for the person who wears either his/her own mask or masks of other subjects that appear in the same database (mask attack accesses). Some samples had to be removed in the mask database due to their improper scans. Finally, in the present study 200 real accesses and 198 mask attack accesses are used for the evaluations.

The mask database is a 2D+3D database. Therefore, for the sake of clarity, the database of real faces in 2D and 3D will be referred as DB-r2 (texture images) and DB-r3 (3D scans) while the database of mask attacks will be referred as DB-m2 and DB-m3 in the rest of this paper. Fig. 2 shows one example from this mask database for a real face and the corresponding mask attack.

III. Reflectance Analysis Based Countermeasure Technique

In this part, initially, we explain how a gray-level image can be decomposed into reflectance and illumination components using the variational retinex algorithm [10]. Next, the classification technique, which uses reflectance components as input, is explained for the purpose of detecting mask spoofing.

A. The Variational Retinex Algorithm

In order to decompose an image into reflectance and illumination components, the variational retinex algorithm explained in the study of Nizar [10] is used, in which it is stated that they examine the variational retinex algorithm proposed by R. Kimmel, D. Shaked, and M. Elad from Hewlett-Packard Laboratories – Israel.

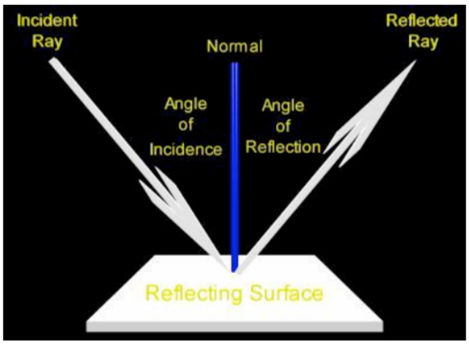

Figure 4. Illustration for the image decomposition. This figure is taken from [10].

According to the study of Nizar [10], our vision ensures that the perceived color of objects remains relatively constant under varying illumination conditions, and this helps us to identify objects. Physics say applying red light on a green apple is not the same as applying white light on the same green apple. In reality, however, we attempt to see the same color, regardless of the applied light. This physical illusion effect is known as the retinex effect.

An image can be considered as a two dimensional function *S(x, y)*, where every point *(x, y)* in the domain is equivalent to 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 it is mentioned in [10], since images are generated from physical processes, the intensity *S* is proportional to the energy radiated by the source. As a consequence, *S(x, y)* must be nonzero and finite ($0 < S(x, y) < \infty$).

Furthermore, the intensity S may be characterized by two components as shown in Fig. 4 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. (1).

$$S(x,y) = L(x,y) \times R(x,y) \tag{1}$$

where $0 < L(x, y) < \infty$ and $0 < R(x, y) < 1$. The reflectance image *R* is bounded by 0 (total absorption) and 1 (total reflectance). From these two inequalities, it is clear that $L(x, y) > S(x, y) > 0$. In this paper, we use the reflectance component *R(x, y)* for the classification of masks and real faces.

In [10], 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. There are several retinex algorithms such as the random walk algorithm, the homomorphic filtering algorithm, the poisson algorithm and the variational retinex algorithm which are explained in [10] briefly. In this study, the variational retinex algorithm is selected to be used to obtain the reflectance component of images which will be used as input by the classifier in the next step of the proposed countermeasure to detect mask spoofing.

In the variational retinex algorithm, the concept of minimizing the energy of a given system is used. For a given image, an energy function is designed and aim is to minimize this energy function. Minimizing energy functions often includes solving partial differential equations. More specifically, we often deal with certain type of equations called: Euler-Lagrange differential equations. As explained in [10], in the Euler-Lagrange problem, we usually have a continuous real-valued function $y = f(x)$ with continuous derivative $y' = df / dx$. Considering *x, y,* and *y'* as three independent variables, we define a new function *g (x, y, y')*. Using this new function, the energy function is defined as: $E = \int g(x, y, y')\, dx$. As it is explained in [10], the energy function *E* has a minimal value if Euler-Lagrange equation:

$$\frac{\partial g}{\partial y} - \frac{\partial}{\partial x}\left(\frac{\partial g}{\partial y'}\right) = 0 \tag{2}$$

is satisfied. The left hand side of this equation is denoted as ∇E. Here *f* is introduced as function of one independent variable *x*, the same concept is applied when *f* is function of *n* independent variables: $x_1, x_2, \dots , x_n$. In particular, when $u = f(x, y)$, function of two independent variables *x*, and *y*, Euler-Lagrange equation becomes:

$$\nabla E = \frac{\partial g}{\partial u} - \frac{\partial}{\partial x}\left(\frac{\partial g}{\partial u_x'}\right) - \frac{\partial}{\partial y}\left(\frac{\partial g}{\partial u_y'}\right) = 0 \tag{3}$$

A first step taken by most algorithms in such kind of problems is the conversion to the logarithmic domain by *s=log (S+1), l=log(L+1),* and *r=log(R+1)*. In the logarithmic domain the relation between these three images becomes: $s=l+r$. Since logarithmic function is monotone increasing, the inequality $l \geq s \geq 0$ still holds. In this study, the problem is also analyzed in the logarithmic domain. As it is explained in [10], the variational retinex algorithm is based on three basic assumptions:

1. The illumination image *l* is spatially smooth. This means the algorithm tries to minimize $\int|\nabla l|^2 dxdy$.
2. The reflectance image *r* is also spatially smooth. This means the algorithm tries to minimize $\int|\nabla(l-s)|^2 dxdy$, *the norm of the gradient of the reflectance r.*
3. We already discussed that $l \geq s$; the variational retinex algorithm goes beyond this assumption and assumes that the illumination image is close to the intensity image. This means the algorithm tries to minimize $\int|(l-s)|^2 dxdy$, *the norm of the reflectance image r.*

These three assumptions mentioned above are combined to define our energy function:

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

where *α* and *β* are positive constants. Since *S* is the given image, *s* here is constant. The integrand is our function

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

Euler-Lagrange equation becomes:

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

which means $\alpha(l-s)-\nabla l-\beta\nabla(l-s)=0$. To solve this equation, the idea of the steepest descent is applied with an auxiliary variable *t* as explained in [10]:

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

The variational retinex algorithm uses this equation to estimate the illumination image *l*. The inequality $l \geq s \geq 0$ must always be satisfied. Finally, the initial value of *l* is taken as the image *s*. After *l* is computed, *r* can be computed from $r = s - l$. Finally the reflectance component *R* is evaluated from $R = e^{r}$ and the illumination component *L* is evaluated from $L = e^{l}$.

In our experiments, we used the values 0.0001 and 0.1 for *α* and *β*, respectively, as suggested in the study of Nizar [10].

B. *The Classification*

Before applying the variational retinex algorithm to decompose the image into illumination and reflectance components, all images are resized to 64×64 normalized pixel image. In [5], we also used this parameter (64×64) to reshape the images this is why we preferred to use the same parameter in this study for comparison purposes. Next illumination and reflectance components are extracted with the variational retinex algorithm, which are also in the same size of 64×64 pixel image. The reflectance and the illumination components of a real face and corresponding mask attack are shown in Fig. 5.

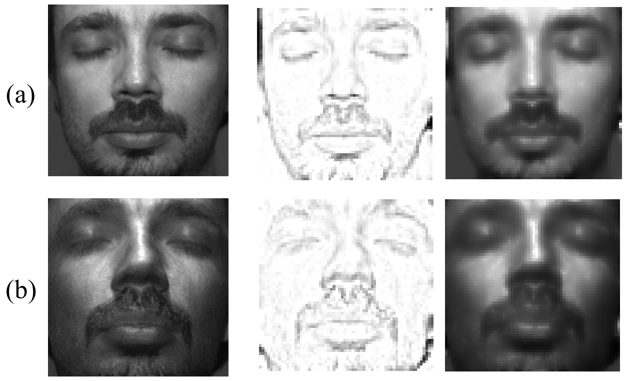

Figure 5. Example from the mask database which is created by [7] (a) The real face with texture, the normalized reflectance image and the illumination image of the real face (b) Same images for the mask of the same person.

After obtaining the reflectance component, which is in the size of [64 64], we reshape the R component as an array of size [1 4096], (64×64=4096), which is our feature vector for the classification. Our observations on the reflectance components of masks and real faces reveal that the reflectance is more for mask samples compared to the real face samples especially at some specific regions of the face. We know that *R* satisfies the inequality *0 < R (x, y) < 1*. *R = 0* means total absorption whereas *R = 1* means total reflectance. The first plot in Fig. 6 shows the mean feature vectors extracted from the *R* components of the mask images and real face images, separately, using the training set of the mask database. This plot shows that for the real face images, we observe more features close to 0 compared to the mask images. This proves that the reflection is less especially at some regions of the face for the real face images. We repeat the same test this time using the test set of the mask database and the results are shown in the second plot of Fig. 6. The test is repeated using the test set since the test and training sets of the mask database are non-overlapping and thus it helps us to make our observation more definite. In the second plot of Fig. 6, different images are used, however similar result to the first plot is obtained. Again the reflectance characteristics of masks and real faces are observed to be different especially at some specific regions of the face.

Based on our observation related to different reflectance characteristics of masks and real faces, we decided to use these feature vectors of length 4096 extracted from the reflectance

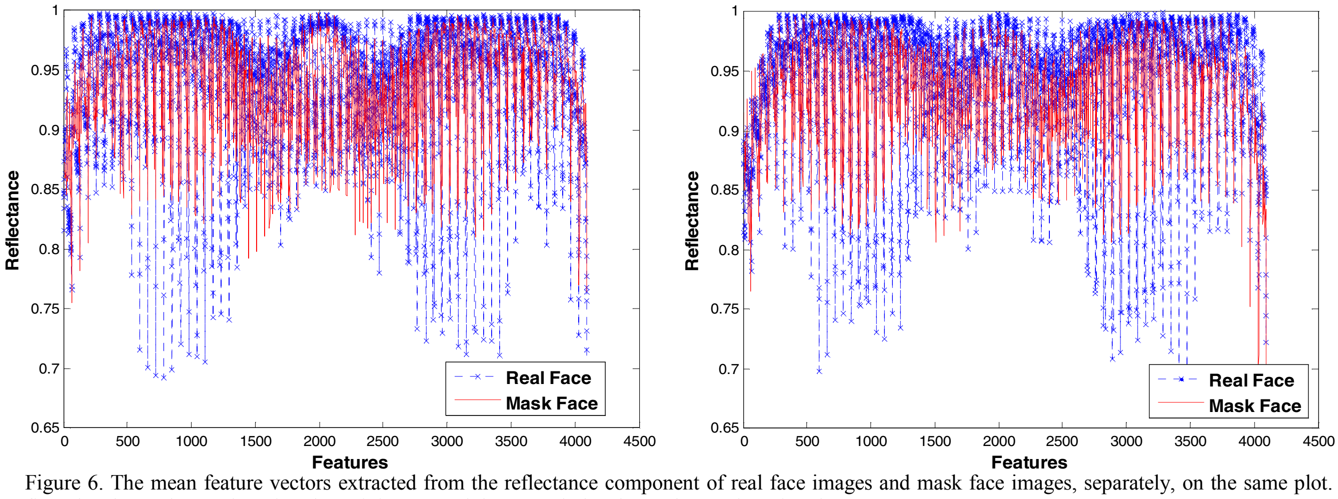

Figure 6. The mean feature vectors extracted from the reflectance component of real face images and mask face images, separately, on the same plot. The first plot shows the results using the training set and the second plot shows the results using the test set.

component of each image as input for our classifier. Finally, linear support vector machine (SVM) classifier [11] is applied.

IV. Experiments and Results

The advantages of the proposed countermeasure can be listed as: easy to implement, robust, does not require user cooperation, computationally fast hence it can be applied in real time, and provides higher performance compared to the existing countermeasures against mask attacks.

For performance evaluation, the mask database which is created by MORPHO [7] is used. Since this is a 2D+3D database, we have both the texture images and the depth maps for the live humans and their masks.

While creating the mask database, the masks and the real faces are with close eyes. Furthermore, the real subjects and the subjects wearing masks look like a static as much as possible by minimizing the movements. Eventually, all eye movements and any facial movements are removed, which makes the spoofing detection problem more challenging.

As mentioned before, in the mask database, 20 subjects appear in total. The masks are manufactured for only 16 of these subjects. Initially, DB-r and DB-m are partitioned in non-overlapping training and test datasets. For DB-r, this is done by randomly selecting 8 subjects out of 16 subjects whose masks are manufactured and by randomly selecting 2 subjects out of 4 subjects whose masks are not manufactured. The samples of selected subjects are assigned to the test set of DB-r, while the rest is used for the training 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 training set of DB-m. Since there is no overlap between the training and the test sets, the spoofing detection problem is more challenging.

The DB-r contains altogether 100 face images of 10 real clients for the training and 100 face images of remaining 10 real clients for the test set. The number of samples in the training and the test sets of DB-m can vary slightly according to the selected subjects for the test and the training sets of DB-r. The reason is that the number of subjects whose mask is manufactured is 16 whereas total number of subjects in the database is 20. The test set of DB-m involves the mask attacks to the corresponding identities in the test set of DB- r and the training set of DB-m involves the remaining mask attacks. Since the number of mask attacks to each corresponding identity is not equal in the mask database, we can have different number of samples for the training and the test sets of DB-m according to the selected subjects for the test set of DB-r. In our test-training partitioning, the DB-m contains 99 mask face images for the training and remaining 99 mask face images for the test set.

A. Evaluation Results

Since there are a few studies about countermeasures for the protection of face recognition systems against mask attacks, similar to the our previous study [5], the experiments are done according to the protocols which are used for photograph spoofing detection in studies reported in [12, 13].

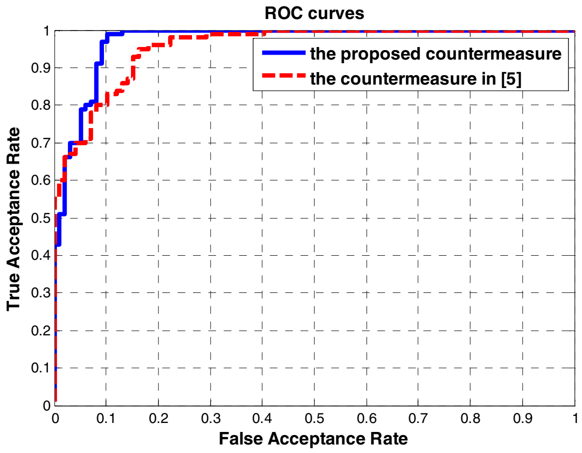

Figure 7. Detection performances of the proposed countermeasure and the countermeasure in [5] using the texture images in the mask database.

Table I. Area Under Curve and Best Accuracy Results Using The Proposed Countermeasure And The Technique In [5] On Both Depth Maps And Texture Images

Techniques	**AUC**	**Accuracy (%)**
Technique in [5] On Texture Images	0.96	89.45
Technique in [5] On Depth Maps	0.92	82.91
The Proposed Countermeasure	**0.97**	**94.47**

In [12, 13], the proposed countermeasures are applied to detect photograph attacks whereas in this study and in our previous study [5], the countermeasures are applied to detect mask attacks using the same protocol.

Table I presents our detection accuracy results using the proposed countermeasure and the technique in [5] on both depth maps and texture images, separately, using the same mask database with the same training-test set partitioning. We also report our results in terms of Area under Curve (AUC) as Tan et al. did in their paper [13]. Fig. 7 shows the detection performance of the proposed countermeasure together with the detection performance of the technique in [5] when it is applied on the texture images. We do not report the results of the technique in [5] when it is applied on the range images in Fig. 7 in order to make the comparison just between the countermeasures which use the 2D data (texture images). The proposed countermeasure is able to achieve satisfactory spoofing detection rate, yielding best classification accuracy of 94.47%, false acceptance rate of 10.1% and false rejection rate of 1%.

As mentioned before in the study of Zhang et al. [4], they achieved 89.18% mean detection accuracy of real face vs. mask face. Since the mask databases used in the experiments are different, we cannot make an exact comparison with the technique in [4]. This is why, our results are compared with the results of our previous approach [5] which use the same mask database with the same test and training sets. The results of the proposed countermeasure are better compared to the results of the technique in [5] as shown in Table I and Fig. 7. However it still needs to be improved. The main reason of the little loss in the accuracy may be that there are less number of samples in the mask database. Therefore the database may not be sufficient enough to test and especially to train the proposed countermeasure. The number of samples in the photograph attack database that is used in the studies [12, 13] is 9123, which is very high compared to the number of samples in our mask attack database. Since there is no publicly available mask attack database, we can only report the performance of the proposed countermeasure using this mask database. However we claim that with increasing number of samples in the database used, better performances can be reached with the proposed countermeasure.

The mask database contains much less samples compared to the photograph database used in the studies [12, 13]. However when we compare the reported AUC and accuracy results in our study and the studies [12, 13], we can say that the proposed countermeasure is very successful to detect mask attacks. AUC is reported as 0.94 in [13] and 0.99 in [12]. Both of the studies [12, 13] use the NUAA photograph database [13]. In this paper, AUC is computed as 0.96 and 0.92 when the countermeasure in [5] is applied on the texture images and the depth maps in the mask database, respectively. In this study, AUC is computed as 0.97 using the same mask database. We can say that the proposed countermeasure gives better results compared to our previous study [5] and the study in [13] and comparable results with the study in [12] although the mask database contain really less number of samples compared to the photograph database.

When we compare the results of the proposed countermeasure and the texture analysis based countermeasure in [5], for which the same mask database is used, it is clear that the reflectance analysis provides even slight more information to detect mask attacks compared to the texture analysis.

V. Conclusions

In this study, a 2D+3D face mask attack database is used which is prepared for the EU research project TABULA RASA [6]. It is used to evaluate the performances of the proposed countermeasure for the protection of face recognition systems against mask attacks.

The novelty of this study is that it is one of the few studies which proposes a countermeasure technique to detect mask attacks. The mask attack database is 2D+3D, however since the proposed countermeasure is a reflectance analysis based technique, it is applied only on 2D texture images in the mask database. The results show that the technique provides satisfactory results to detect mask spoofing. Existing 3D scanners provide also texture images. Therefore, the proposed countermeasure can be used to protect both 2D and 3D FR systems against mask attacks.

The proposed countermeasure is a reflectance analysis based approach, which benefits from the variational retinex algorithm [10] to decompose the image into reflectance and illumination components. After obtaining the reflectance component of images, linear SVM classifier is applied to the feature vectors extracted from these reflectance components. The result of the classification step proves that masks and real faces have different reflectance characteristics especially at some specific regions of the face, hence it provides significant advantage to detect mask attacks using reflectance analysis. In this paper, a classification accuracy of 94.47% is achieved for real face vs. mask face.

Standard face recognition systems are not robust to the spoofing attacks therefore robust algorithms are necessary to mitigate the effects of spoofing attacks. Up to now, we have achieved satisfactory results to detect mask attacks. Our future work is to apply fusion of different countermeasures to obtain better results. Furthermore, we plan to test the proposed countermeasure on a 2D face attack (photograph or video) database to observe if we can also obtain satisfactory results to detect 2D face attacks using the proposed countermeasure.

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] 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, pp. 1-6.

[2] J. Maatta, A. Hadid, M. Pietikainen, “Face spoofing detection from single images using texture and local shape analysis,” in IET Biometrics, vol. 1, March 2012, pp. 3–10.

[3] N. Kose, J.-L. Dugelay, “Classification of Captured and Recaptured Images to Detect Photograph Spoofing,” IEEE IAPR International Conf. on Informatics, Electronics & Vision, ICIEV, May 2012, pp. 1027-1032.

[4] Z. Zhang, D. Yi, Z. Lei, S. Z. Li, “Face Liveness Detection by Learning Multispectral Reflectance Distributions”, IEEE International Conference on Automatic Face & Gesture Recognition and Workshops (FG 2011), March 2011, pp. 436-441.

[5] N. Kose, J.-L. Dugelay,, “Countermeasure for the Protection of Face Recognition Systems Against Mask Attacks,” IEEE International Conference on Automatic Face & Gesture Recognition and Workshops (FG 2013), in press.

[6] http://www.tabularasa-euproject.org/.

[7] http://www.morpho.com/

[8] http://www.thatsmyface.com/Products/products.html

[9] http://www.sculpteo.com/en/

[10] N. Almoussa, “Variational Retinex and Shadow Removal”, Technical Report, The Mathematics Department – UCLA.

[11] C.-C. Chang and C.-J. Lin, “LIBSVM : a library for support vector machines,” ACM Transactions on Intelligent Systems and Technology, 2:27:1--27:27, 2011.

[12] J. Maatta, A. Hadid, M. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” Proc. of IAPR IEEE Int. Joint Conf. on Biometrics (IJCB), Washington DC, USA, 2011, pp. 1-7.

[13] X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from a single image with sparse low rank bilinear discriminative model,” Proc. of the 11th European Conf. on Computer vision: Part VI, ECCV'10, Berlin, Heidelberg, 2010, pp. 504-517