Countermeasure for the Protection of Face Recognition Systems Against Mask Attacks

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

Abstract— **There are several types of spoofing attacks to face recognition systems such as photograph, video or mask attacks. Recent studies show that face recognition systems are vulnerable to these attacks. In this paper, a countermeasure technique is proposed to protect face recognition systems against mask attacks. To the best of our knowledge, this is the first time a countermeasure is proposed to detect mask attacks. The reason for this delay is mainly due to the unavailability of public mask attacks databases. In this study, a 2D+3D face mask attacks database is used which is prepared for a research project in which the authors are all involved. The performance of the countermeasure is evaluated on both the texture images and the depth maps, separately. The results show that the proposed countermeasure gives satisfactory results using both the texture images and the depth maps. The performance of the countermeasure is observed to be slight better when the technique is applied on texture images instead of depth maps, which proves that face texture provides more information than 3D face shape characteristics using the proposed approach.**

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 an access to the system. Based on the observations that face recognition systems are vulnerable to spoofing attacks, researchers started to work on countermeasures to reduce the impact of spoofing attacks on recognition performances. Recently, there have been studies on 2D face countermeasures to detect photograph and video spoofing [1 - 3]. However, the topic of mask spoofing attacks to face recognition systems is considerably new. The main reason for this delay is due to the unavailability of public mask attacks databases. This paper aims to fill this gap by proposing a countermeasure technique to protect face recognition systems against mask spoofing using the mask database which is prepared within the context of a European Union (EU) research project.

The preparation of mask spoofing database is much more difficult and expensive than the preparation of photograph or video spoofing databases. This is why there is still a gap in the areas which analyze the impact of mask spoofing attacks on face recognition (FR) systems and the countermeasure techniques to reduce these impacts.

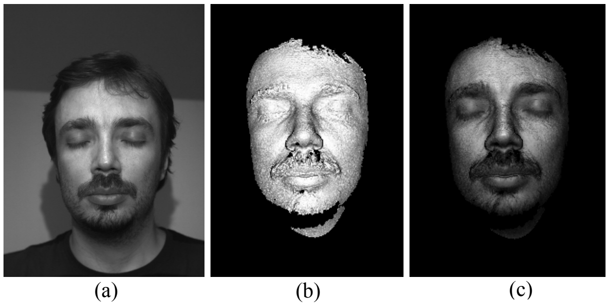


Figure 1. Example from the mask attacks database created by [5] (a) Texture image (the default output of most existing 3D scanners) (b) the snapshot of 3D scan (the default output of 3D scanners) (c) the snapshot of the 3D scan with texture that is obtained when the texture image (a) is mapped on the 3D scan (b).

In the present study, our aim is to reduce the impact of mask attacks on the performances of face recognition systems by applying a local binary patterns (LBP) based countermeasure technique.

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. On the other hand, depth maps are estimated from 3D scans, therefore countermeasure which is developed by using only the depth maps can be used to protect 3D FR systems since these scans can be obtained only by using 3D scanners.

In this study, the proposed countermeasure do not need any extra hardware and user collaboration. The technique relies on a single image. The mask attacks database which is used in this

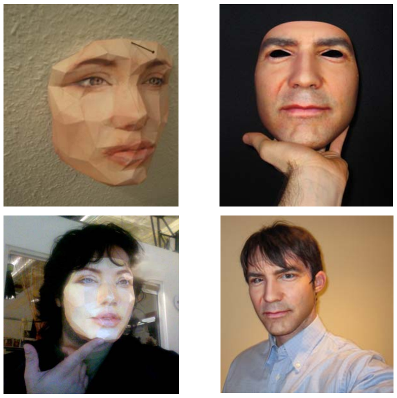


Figure 2. (upper row) Example samples for paper and fabric masks, (lower row) Masks in the upper row which are worn on the face. The pictures are taken from [4].

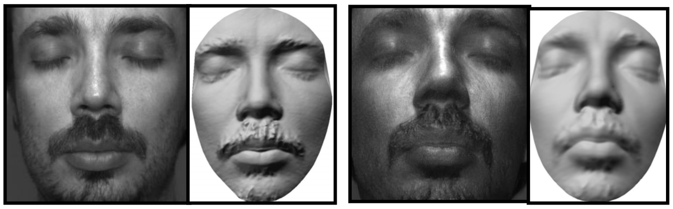
study was created by MORPHO [5]. Since the database includes many high quality mask samples, it provides significant advantage to evaluate the performance of the proposed countermeasure to detect mask attacks.

In this paper, the countermeasure technique is applied on both the texture images and the depth maps (range images), separately. The texture images used in this study are the default outputs of the scanner which was used by [5] while creating the mask database. On the other hand, the depth maps used in this study are estimated from the 3D scans which are provided by the mask database.

The novelties of our study can be listed as follows:

- The countermeasure technique which is explained in [7] is used to detect 2D face print (e.g. photograph, face picture on a paper) attack whereas in this study we use this technique to detect mask attack, which is a 3D face attack.
- In this study, for the protection of 3D FR systems against mask attacks, the initial aim was to use only the 3D data to propose a countermeasure. However, existing 3D scanners provide also texture images, hence in this study we also apply the countermeasure on the texture images. The reason is that 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.
- In [7], the technique is applied on the texture images of the photograph database whereas in this study, it is applied on both the texture images and the corresponding depth maps of the mask database. Therefore with this study, we are able to test that this countermeasure can be applied also on depth maps, which provides a solution to protect 3D FR systems against mask attacks using only the 3D data.
- To the best our knowledge, it is the first time a countermeasure is proposed to detect mask attacks.

In this paper, the results are shown in two parts: evaluation results on the texture images (2D data) and evaluation results on the depth maps (3D data). The results show that the proposed countermeasure is successful to detect mask attacks using both the texture images and the depth maps in the mask database.



(a) (b)

Figure 3. Example from the mask database which is created by [5] (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.

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.

There are several ways of mask manufacturing. A mask of a person can be prepared even by using papers (Fig. 2). The company 'Thats My Face' [4] provides colored masks. It needs one frontal and one profile picture of the target person. For each ethnicity, the company has a standard 3D face model and masks are manufactured by mapping the 2D pictures (one frontal and one profile picture) of the target person on the 3D face model which shows the ethnic characteristics of the target person. However, since the 3D model is based on an ethnic shape, it does not show the exact 3D face shape characteristics of the target person. Mask samples using paper and using 2D pictures of the target face are shown in Fig. 2, respectively.

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 use a structured light technology. Then the 3D mesh was obtained for each subject, which is the projection of the acquisition into a polygon 3D model. In the final step, each 3D model was sent to the 3D printer and masks were manufactured by Sculpteo 3D Printing [6].

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, 10 scans are taken for the original person (real accesses) and almost 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). This means that in the mask database, there are 200 acquisitions for the real accesses and almost 200 acquisitions for the mask attack accesses.

Fig. 3 shows one example from this mask database for a real face and the corresponding mask attack.

III. LBP Based Countermeasure Technique To Detect Mask Attacks

Nowadays spoofing is a popular topic. Therefore up to now, several studies on countermeasures have been published. There are studies on countermeasures to detect 2D face attacks such as photograph and video spoofing, however to the best of our knowledge, this is the first time that a countermeasure is proposed to detect mask spoofing.

In the study of J. Maatta et. al [7], they provide a texture analysis approach to detect 2D face print attacks. Face prints usually contain printing quality defects that can be well detected using texture features. In [7], they presented an approach based on analyzing facial image textures to detect whether there is a live person in front of the camera or a face print. This approach analyses the texture of the facial images using multi-scale local binary patterns (LBP).

The results reported in [7] show that the approach is very successful to detect face print attacks. In our study, the aim is to detect mask attacks. Mask database which is used in this study is a very high quality database which means that the masks are very similar to the corresponding real faces (Fig. 3). However, a close look at the differences between masks and real faces reveals that they have different texture and smoothness characteristics. Based on these observations, the LBP based approach in [7] is preferred to be used for this study this time in order to detect mask attacks.

A. Pre-processing

There are slight alignment differences between the faces in the mask database. Therefore initially, all 3D faces in the mask database are aligned to a generic face for this study. This process makes the alignment of all faces identical.

The purpose of the pre-processing in 3D FR is to crop the face region, to eliminate the spikes and the holes and to smooth the facial surface which increase the performances of recognition techniques. However 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 raw data is preferred to be used. The depth maps are estimated from the raw aligned 3D scans. Only 2D cropping is applied to extract the face region from both the texture images and the corresponding depth maps. Then all images are resized into 64×64 grayscale image.

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 (estimated depth maps from the 3D scans) while the database of mask attacks will be referred as DB-m2 and DB-m3 in the rest of this paper.

B. Brief Information on Spoofing Detection using Micro-Texture Analysis

In [7], the countermeasure is explained in details. In this part, a brief information is given to explain the technique which is also used in this paper. The same technique in [7] is applied in this study, however this time to protect FR systems against mask attacks instead of photograph attacks.

Captured image from mask may visually look very similar to the image captured from live face (e.g. the texture images in Fig. 3). All these images would be largely overlapping in the original input space. Therefore a suitable feature space is necessary to separate the real faces and masks when the texture images are used as input data.

A close look at the differences between real faces and masks reveals that their surface properties are different. In addition, for mask manufacturing 3D printers are used, hence they may contain printing quality defects that can be detected with micro-texture patterns. Therefore, in the first part of the experiments of this study, the countermeasure is applied on the texture images (DB-r2 and DB-m2) to test if different texture characteristics of masks and real faces provide enough information to detect mask attacks.

The 3D shape of high quality mask is also very similar to the 3D shape of corresponding real face (e.g. the 3D scans whose snapshots are shown in Fig. 3). Therefore the depth maps of real faces and corresponding mask attacks are very similar which means that again, a suitable feature space is necessary to separate the real faces and masks when the depth maps are used as input data.

Our analysis on the 3D mask database 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 mask, the 3D scan of the mask is smoother in these parts compared to the real face scan. The real face contains facial hair this is why the parts of the face with facial hair are rough and there are usually holes on the real face scan in these parts (Fig. 1). Of course, high quality scanners cause less number of holes however even with the best scanners it is possible to observe some holes on the scan especially at the parts with facial hair. Therefore, in the second part of the experiments, the countermeasure is applied on the depth maps which are estimated from the raw scans (DB-r3 and DB-m3) to test if different 3D face shape and different smoothness characteristics of masks and real faces provide enough information to detect mask attacks.

The LBP based countermeasure technique emphasizes the micro-texture differences in the feature space. It aims at learning the fine differences between real face and fake face, and then designs a feature space which emphasizes those differences. In this study, the vectors in the feature space are then fed to an SVM classifier which determines whether the micro-texture patterns characterize a real face or a mask face.

The method in [7] adopts LBP, which is a powerful texture operator, for describing not only the micro-textures but also their spatial information.

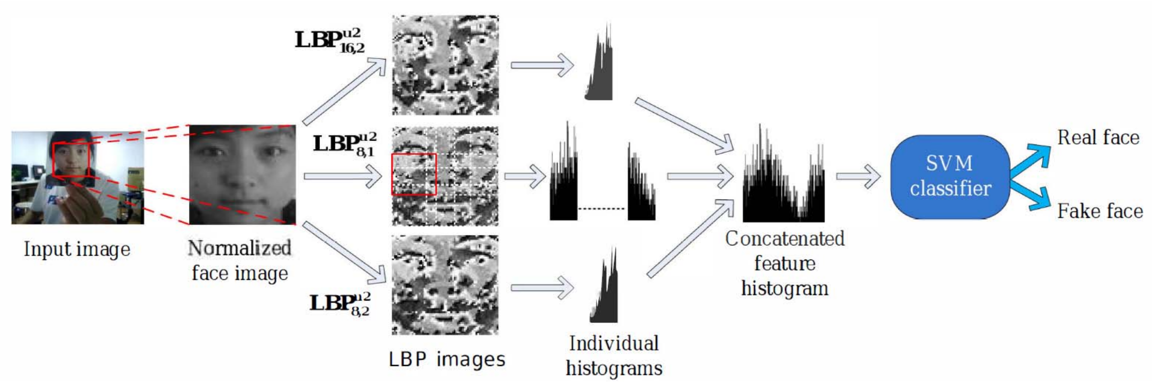


Figure 5. The countermeasure technique that is used to detect mask attacks. The figure is taken from [7].

The LBP texture analysis operator, introduced by Ojala et al. [8], is defined as a gray-scale invariant texture measure, derived from a general definition of texture in a local neighborhood. The advantages of the technique are its power in terms of texture description, computational simplicity and tolerance against monotonic gray-scale changes.

The original LBP operator forms labels for the image pixels by thresholding the 3 x 3 neighborhood of each pixel with the center value and considering the result as a binary number. Fig. 4 shows an example of a LBP calculation. The histogram of these $2^8 = 256$ different labels can then be used as a texture descriptor.

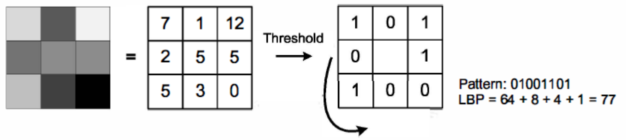


Figure 4. An example for LBP calculation. The figure is taken from [7].

The 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 neighbours. In Equation (1), g_c is the gray value of the central pixel, g_p is the value of its neighbours, P is the number of neighbors around a circle of radius R. $LBP_{P,R}$ is calculated as follows using Equations (1) and (2) :

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

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \tag{2}$$

Another extension to the original operator is the use of uniform patterns. 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 for the uniform LBP operator is $LBP_{P,R}^{u2}$. Superscript u2 stands for using only uniform patterns and labeling all remaining patterns with a single label.

The occurrences of the LBP codes in the image are usually collected into a histogram. The classification can be then performed by computing histogram similarities. For an efficient representation, facial images are first divided into several local regions from which LBP histograms are extracted and concatenated into an enhanced feature histogram. In [7], their investigations have shown that micro-texture details that are needed to discriminate a real human face from fake ones can best be detected using a combination of different LBP operators. Therefore, to better capture the differences between real human faces and fake ones, they derive an enhanced facial representation using multi-scale LBP operators. The proposed representation is shown in Fig. 5. As illustrated in Fig. 5, their proposed representation computes LBP features from 3 x 3 overlapping regions to capture the spatial information and enhances the holistic description by including global LBP histograms computed over the whole face image. This is done as follows: the face is first cropped and normalized into a 64 x 64 pixel image. Then, they apply $LBP_{8,1}^{u2}$ operator on the face image and divide the resulting LBP face image into 3 x 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 $LBP_{8,2}^{u2}$ and $LBP_{16,2}^{u2}$ operators, yielding 59-bin and 243-bin histograms that are added to the 531-bin histogram previously computed. Hence, the length of the final enhanced feature histogram is 833 (i.e. 531 +59+243).

Once the enhanced histograms are computed as explained in [7], a linear SVM classifier [9] is used in our study to determine whether the input image corresponds to a live face or not. The SVM classifier is first trained using a set of positive (real faces) and negative (masks) samples.

IV. Experiments and Results

For performance evaluation, the mask database which is created by Morpho [5] 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

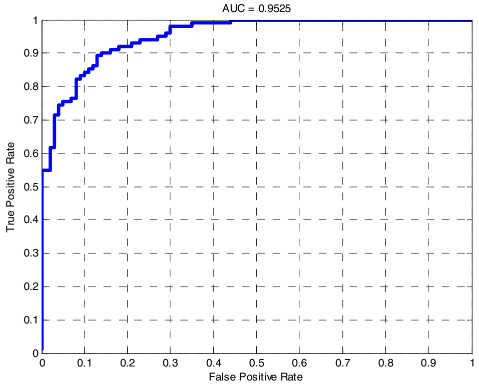


Figure 6. Detection performance of the countermeasure using the texture images in DB-r2 and DB-m2.

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.

To the best of our knowledge, it is the first time a countermeasure technique is proposed to detect mask attacks. Therefore, in the evaluations we could only show our results without including any comparison with other techniques.

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. There is no overlap between the training and the test sets which makes the spoofing detection problem more challenging. This training-test set partitioning is done for both the texture images and the corresponding depth maps.

Table I shows the number of samples in the training and the test sets of each database. 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 and DB-r are different. 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. Therefore, the number of samples in the training and the test sets of DB-m can vary according to the selected subjects for the test set of DB-r.

TABLE I. TRAINING – TEST SET PARTITIONING IN 2D AND 3D FOR DB-R AND DB-M

# of Samples	DB-r2	DB-m2	DB-r3	DB-m3
Training Set	100	105	100	105
Test Set	100	99	100	99

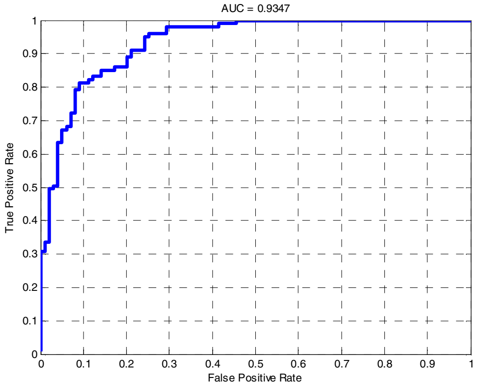


Figure 7. Detection performance of the countermeasure using the depth maps in DB-r3 and DB-m3.

A. *Evaluation Results on the Texture Images*

Since there are no other studies about countermeasures for the protection of face recognition systems against mask attacks, the experiments are done according to the protocols which are used for photograph spoofing detection in the studies [7, 10]. In [7], the proposed countermeasure is applied on the texture images of photographs whereas in this part, it is applied on the texture images of masks to test if the technique is also successful to detect mask attacks.

Table II presents our results using the texture images in DB-r2 and DB-m2. We also report our results in terms of Area under Curve (AUC) as Tan et al. did in their paper [10]. Fig. 6 shows the detection performance of the proposed countermeasure using the texture images. The method is able to achieve satisfactory spoofing detection rate, yielding total classification accuracy of 88.12% , false acceptance rate of 14% and false rejection rate of 9.8%.

B. *Evaluation Results on the Depth Maps*

Since there are no other studies about countermeasures for the protection of 3D face recognition systems against mask attacks, in this part, we evaluate our results according to the protocol which is used for Part A of Section IV.

The same protocol is used for the evaluations on both the texture images and the depth maps, therefore we can compare the results of Part A and Part B in order to have an idea of whether the technique is better on 2D or 3D data.

Table II also presents our results using the depth maps in DB - r3 and DB - m3. Again AUC is computed for this

TABLE II. AREA UNDER CURVE AND BEST ACCURACY RESULTS USING THE TEXTURE IMAGES AND THE DEPTH MAPS

Countermeasure Applied on	AUC	Accuracy (%)
Texture Images	0.9525	88.1
Depth Maps	0.9347	86.0

experiment and reported in Table II. Fig. 7 shows the detection performance of the proposed countermeasure using the depth maps. The method was able to achieve satisfactory spoofing detection rate, yielding total classification accuracy of 86%, false acceptance rate of 9.1% and false rejection rate of 18.8%.

According to the results reported in Table II, we can say that the proposed countermeasure provides satisfactory results using both the texture images and the depth maps. However, the performance of the countermeasure is observed to be slight better when the technique is applied on texture images instead of depth maps, which proves that face texture provides more information than 3D face shape characteristics using the proposed countermeasure.

The results can be considered as satisfactory, however they still need to be improved. The main reason of lower accuracy is that there are less number of samples in the mask database. Therefore the database is not sufficient enough to test and especially to train the proposed countermeasure. The number of samples in the photograph attack database which is used in the studies [7, 10] is 9123 whereas our mask database includes only 404 samples, which is very less compared to the photograph 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 whether it is applied on the texture images or the depth maps.

The mask database contains much less samples compared to the photograph database used in the studies [7, 10]. However when we compare the reported AUC and accuracy results in our study and the studies [7, 10], we can say that the proposed countermeasure is very successful to detect mask attacks using either the texture images or the depth maps. AUC is reported as 0.94 in [10] and 0.99 in [7]. Both of the studies [7, 10] use the texture images in the photograph database. In our study, AUC is computed as 0.95 and 0.93 using the texture images and the depth maps, respectively, in the mask database. We can say that the proposed countermeasure gives comparable results with the studies [7, 10] although the mask database contain really less number of samples compared to the photograph database.

V. Conclusions

In this study, a 2D+3D face mask attack database is used which is prepared for a EU research project. 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 the first time that a countermeasure technique is proposed to detect mask attacks. The mask attack database is 2D+3D, therefore the proposed countermeasure is applied on both 2D and 3D data. The results show that the technique provides satisfactory results on both the texture images and the depth maps. Since the technique is successful using both 2D and 3D data, it provides significant advantage to protect both 2D and 3D face recognition systems.

The proposed countermeasure is an LBP based approach. LBP based approaches are generally applied on texture images. Even there is an increase in the studies which apply LBP on the depth maps, it is not as common as the case for the texture images. The results in our study show that the LBP based countermeasure provides also very satisfactory results when the technique is applied on depth maps. Standard face recognition systems are not robust to the spoofing attacks therefore robust algorithms are necessary to mitigate the effects of spoofing attacks. Countermeasure techniques have to be developed to make the systems robust to mask attacks. Our future work is to develop novel countermeasure techniques which provide even better classification accuracies in order to detect mask spoofing.

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.

[2] 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.

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

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

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

[7] J. Maatta, A. Hadid, and 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.

[8] T. Ojala, M. Pietikainen, and T. Maenpaa. “Multiresolution gray-scale and rotation invariant texture classification with local binary patterns,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, pp. 971-987, July 2002.

[9] 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.

[10] 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, pp. 504-517, Berlin, Heidelberg, 2010