Image and Vision Computing 32 (2014) 779–789

Contents lists available at ScienceDirect

Image and Vision Computing

journal homepage: www.elsevier.com/locate/imavis

Mask spoofing in face recognition and countermeasures☆

Neslihan Kose *, Jean-Luc Dugelay

Multimedia Department, EURECOM, Sophia-Antipolis, France

ARTICLE INFO

Article history:
Received 11 June 2013
Received in revised form 2 May 2014
Accepted 26 June 2014
Available online 4 July 2014

Keywords:
Spoofing
Mask attacks
Countermeasure
Face recognition

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.

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 is 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 in 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

☆ This paper has been recommended for acceptance by Stan Sclaroff.

* Corresponding author.
E-mail addresses: neslihan.kose@eurecom.fr (N. Kose), jean-luc.dugelay@eurecom.fr (J.-L. Dugelay).

http://dx.doi.org/10.1016/j.imavis.2014.06.003
0262-8856/© 2014 Elsevier B.V. All rights reserved.

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 requirements 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 [15,18,17].

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 that 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 that 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 the 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 [15,18,17]. 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 has 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 was 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 appear in the same database was acquired. Finally, 200 real face acquisitions from 20 subjects and 198 mask acquisitions from 16 masks are used for the evaluations of this study. Fig. 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)