

Improving Face Anti-Spoofing by 3D Virtual Synthesis

Jianzhu Guo^{*1,2}, Xiangyu Zhu^{*1}, Jinchuan Xiao^{1,2}, Zhen Lei¹, Genxun Wan³, Stan Z. Li¹

¹National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences

²University of Chinese Academy of Sciences

³First Research Institute of the Ministry of Public Security of PRC

{jianzhu.guo, xiangyu.zhu, jinchuan.xiao, zlei, szli}@nlpr.ia.ac.cn, friwan@163.com

Abstract

Face anti-spoofing is crucial for the security of face recognition systems. Learning based methods especially deep learning based methods need large-scale training samples to reduce overfitting. However, acquiring spoof data is very expensive since the live faces should be reprinted and re-captured in many views. In this paper, we present a method to synthesize virtual spoof data in 3D space to alleviate this problem. Specifically, we consider a printed photo as a flat surface and mesh it into a 3D object, which is then randomly bent and rotated in 3D space. Afterward, the transformed 3D photo is rendered through perspective projection as a virtual sample. The synthetic virtual samples can significantly boost the anti-spoofing performance when combined with a proposed data balancing strategy. Our promising results open up new possibilities for advancing face anti-spoofing using cheap and large-scale synthetic data.

1. Introduction

Due to the intrinsic distinctiveness and convenience of biometrics, biometric-based systems are widely used in our daily life for person authentication. The most common applications cover phone unlock (iPhone X), access control, surveillance, and security. Face, as one of the biometric modalities, gains increasing popularity in academic and industry community. Face recognition has achieved great success in terms of verification and identification, such as Labeled Faces in the Wild (LFW) [15], YouTube Faces DB (YFD) [36] and MegaFace [16]. However, spoof faces can be easily obtained by printers (i.e., print attack) and digital camera devices (i.e., replay attack). These spoofs can be very similar to genuine faces in appearance with proper handlings, like bending and rotating. Therefore, it is important to equip the face recognition system with robust presentation attack detection (PAD) algorithms.

^{*}Equal contribution.

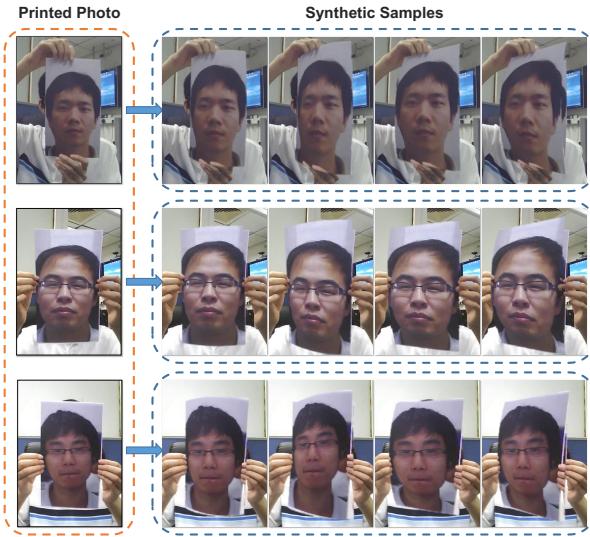


Figure 1: Virtual synthetic samples from CASIA-MFSD. Left column: the original printed photos. Right column: synthetic samples with different vertical/horizontal bending and rotating angles. These synthetic samples can significantly improve the face anti-spoofing performance.

Print and replay attacks are the most common presentation attack (PA) ways and have been well studied in the academic field. Prior works can be roughly divided into three categories: cue-based, texture-based and deep learning based methods. Cue-based methods attempt to detect liveness motions [25, 26] such as eye blinking, lip, and head movements. Texture-based methods aim to exploit discriminative patterns between live and spoof faces, by adopting hand-crafted features such as HOG [17, 7], LBP [6, 39]. Deep learning based methods mainly consist of two types. The first one treats PA as a binary classification or pseudo-depth regression problem [19, 39, 1]. The other one tries to utilize temporal information of the video, such as applying the RNN-based structure [37, 21].

In practical applications, the replay attack can be easily detected using specialized sensors like depth or Near In-

fraRed (NIR) cameras, because the captured depth values of the spoof face lie in one flat surface, which is easily distinguished from live faces. While for the print attack, an imposter will try his best to fool the system, such as bending and rotating the printed photo. However, most of the published databases miss the transformations, so that the trained models are easily spoofed by photo bending and rotating.

On the other hand, learning based methods especially deep learning based methods for face anti-spoofing need a large number of training samples to reduce overfitting. However, it is very expensive to acquire spoof data since the live faces should be re-printed and re-captured in many views. It is worth to note that, several recent works [13, 34, 23, 20] have shown that synthesized images are effective for training CNN-based models in various tasks.

Motivated by these previous works, we propose to address these issues in a virtual synthesis manner. First, the high-fidelity virtual spoof samples with bending and out-of-plane rotating are synthesized through rendering from the transformed mesh in 3D space. Several synthetic examples are shown in Fig. 1. Second, deep models are trained on these synthetic samples with a data balancing method. To validate the effectiveness of our method, we design our experiments in two aspects: intra-database and inter-database testing. The intra-database testing is evaluated on CASIA-MFSD [40] and Replay-Attack [5] for fair comparisons with other methods. For inter-database testing, we choose CASIA-MFSD [40] as our training dataset and CASIA-RFS [18] as our testing set, since CASIA-RFS contain rotated and bent spoof faces series, which is more challenging. Besides, we rebuild the protocol on CASIA-RFS for better quantitative comparisons.

The main contributions of our work include:

- A virtual synthesis method to generate bent and out-of-plane rotated spoofs is proposed. Large scales of spoof training data can be generated for training deep neural networks.
- To train CNN from the large-scale synthetic spoof samples, a data balancing method is proposed to improve generalization of the face anti-spoofing model.
- We achieve the state-of-the-art performances on the CASIA-MFSD and Replay-Attack databases and obtain great improvement of generalization on the CASIA-RFS database.

The remaining of this work is organized as follows. Sec.2 reviews related work. Sec.3 presents our approach for synthesizing spoof data. In Sec.4, we describe our network training and balancing methods for virtual synthetic data. Sec.5 reports experiments. We conclude in Sec.6.

2. Related Work

We review related works from two perspectives: CNN-based methods for face anti-spoofing and data synthesis for CNN training.

CNN-based Methods for Face Anti-spoofing. Many CNN-based methods for face anti-spoofing have been recently proposed, which can be categorized into two groups: texture-based methods [19, 26, 9, 19, 38] and series-based methods [9, 37, 21].

Most of the texture-based methods treat face anti-spoofing as a binary classification problem. In [19, 26], it uses the CaffeNet or VGG model pre-trained on ImageNet as initialization and then fine-tunes it on face-spoofing data. The SVM is finally applied for face spoofing detection. In [9, 19], different kinds of face features (e.g., multi-scale faces or hand-crafted features) are designed to feed into CNN. Nagpal et al. [24] examine the effect of different network architectures (Inception and ResNet) and hyper-parameters on face anti-spoofing performance. Recently, several studies [1, 21, 35] reveal that the depth supervised based methods perform better than binary supervised. Atoum et al. [1] propose to use the pseudo-depth map as supervised signals. A novel two-stream CNN-based approach for face anti-spoofing by extracting the local features and holistic depth maps from the face images is proposed. The fusion of the scores of two-stream CNNs leads to the final predicted class of live vs. spoof. Liu et al. [21] fuse the estimated depth and the rPPG signals to distinguish live vs. spoof faces. They argue that auxiliary supervision such as pseudo-depth map and rPPG signals are important to guide the learning toward discriminative and generalizable cues. The most recent work [35] proposes a depth supervised face anti-spoofing model in both spatial and temporal domains thus more robust and discriminative features can be extracted to classify live and spoof faces.

Series-based methods aim to fully utilize the temporal information of serialized frames. Feng et al. [9] feed both optical flow map and Shearlet feature to CNN. The work [37] proposes a deep neural network architecture combining Long Short-Term Memory (LSTM) units with CNN. In [10], 3D convolution network is adopted in short video frame level to distinguish live vs. spoof face. Besides, the rPPG signals extracted from serialized frames are used as auxiliary supervision for classification in [21].

Virtual Synthesis for CNN Training. Generally, CNN-based methods need a large scale of training data to reduce overfitting. However, training data is difficult to collect in many cases. Several recent works focus on creating synthetic images to augment the training data, *e.g.* face alignment [42, 41], face recognition [13], 3D human pose estimation [4, 8, 11, 32], pedestrian detection [29, 28] and action recognition [30, 31]. Zhu et al. [42, 41] attempt to utilize 3D information to synthesize face images in large

poses to provide abundant samples for training. Similarly, Guo et al. [13] synthesize high-fidelity face images with eyeglasses as training data based on 3D face model and 3D eyeglasses and achieve better face recognition performance on real eyeglass face testset. Pishchulin et al. [28] generate synthetic images with a game engine. In [29], they deform 2D images with a 3D model. In [30], action recognition is addressed with synthetic human trajectories from MoCap data.

3. 3D Virtual Synthesis

In this section, we demonstrate how to synthesize virtual spoof face data. The purpose of synthesis is trying to simulate the behaviors of bending and out-of-plane rotating.

3.1. 3D Meshing and Deformation

We assume that a printed photo has a simple 3D structure, which is a flat surface so that we can easily transfer the printed photo to a 3D object and manipulate its appearance in 3D space. First, we label four corner anchors (Fig. 2(a)) to crop the printed photo region. Second, the anchors are uniformly sampled on cropped region (Fig. 2(b)). Their depths are set the same since we treat the printed photo as a plane. Finally, the delaunay algorithm is applied to triangulate these anchors to mesh the printed photo into a virtual 3D object (Fig. 2(c)). The 3D view of virtual 3D printed photo is shown in Fig. 2(d) and Fig. 2(e).

After 3D meshing, the 3D transformation operations such as rotating and bending can be applied. We use a rotation matrix R to rotate the 3D object. Let V_{xyz} representing the sampled anchors, the rotating operation can be represented by $V = R * V_{xyz}$.

The bending operation involves non-rigid transformation. In order to simulate the bending operation, we deform the 3D planar mesh to a cylinder, with the length along the horizontal and vertical directions preserved. As is shown in Fig. 3, the bending angle θ measures the degree of vertical bending. We show the 2D aerial view of vertical bending in Fig. 4, P is an anchor point on original 3D planar mesh and P' is the deformed anchor point on cylinder surface. The radius of the circle on cylinder mesh surface can be first calculated by $r = l/\theta$, where l denotes the width of 3D planar mesh. The radian of arc $P'C'$ can be calculated by $\phi = d/l \cdot \theta$, where $d = x - l/2$ is the distance from anchor point P to the mesh center C (or from P' to C'). The new position of anchor P' can be formulated as follows:

$$\begin{aligned} x'_\theta &= r \sin \phi = \frac{l}{\theta} \cdot \sin \left(\frac{x - l/2}{l} \cdot \theta \right), \\ z'_\theta &= r \cos \phi - r \cos \frac{\theta}{2} \\ &= \frac{l}{\theta} \cdot \left[\cos \left(\frac{x - l/2}{l} \cdot \theta \right) - \cos \frac{\theta}{2} \right], \end{aligned} \quad (1)$$

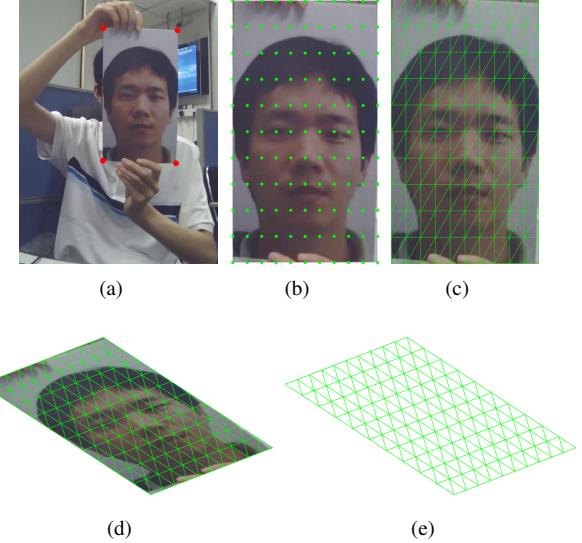


Figure 2: 3D Image Meshing. (a) The input source image marked with corner anchors. (b) The cropped image and sampled anchors. (c) The triangle mesh overlapped with the cropped image (2D view). (d) The triangle mesh overlapped with cropped image (3D view) (e) 3D view of the triangle mesh.

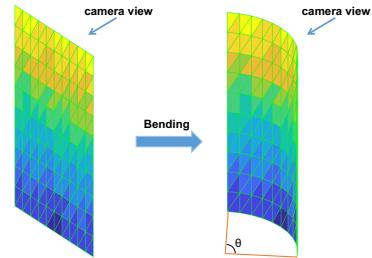


Figure 3: Vertical bending of the planar triangle mesh. Left is 3D planar mesh and right is 3D bending mesh.

where θ is the bending angle. Horizontal bending is similar to vertical bending. Besides, the rotating and bending can be composed to synthesize more varied samples.

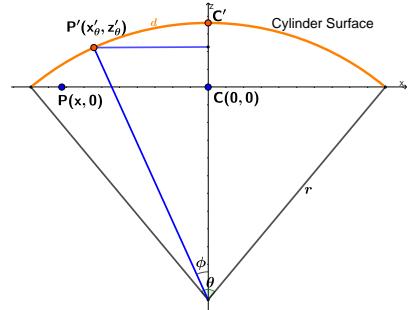


Figure 4: 2D aerial view of vertical bending.

3.2. Perspective Projection

When a printed photo is captured, the texture in the distance should appear smaller than the texture close by. However, this effect is always ignored and the weak perspective projection is adopted in many virtual synthesis techniques [13, 41]. In this work, we use perspective projection for more realistic synthesis.

To perform the perspective transformation, we must first approximate the physical size of the printed photo. We assume the pixel distance and real distance between two eyes centers as d_p and d_r respectively, then the scale factor of the transformation from image space to world coordinated system can be approximated as:

$$s = d_p/d_r, \quad (2)$$

where s is the scale factor of transformation from image space to world coordinate system. Then perspective projection can be applied by

$$\begin{aligned} b_x &= v_x \cdot (f/d_z), \\ b_y &= v_y \cdot (f/d_z), \end{aligned} \quad (3)$$

where f is the focal length, d_z indicates the physical depth distance from camera to photo, v_x, v_y are anchor vertices in world coordinate system, and b_x, b_y are projected 2D vertices by perspective transformation. For convenience, the real distance between eyes centers d_r , the focal length f and the depth d_z are approximated by constant values based on prior.

After the mesh deformation and projection, synthetic samples can be rendered by Z-buffer. Fig. 5 shows the difference between weak perspective projection and perspective projection. The image synthesized by perspective projection in Fig. 5(c) is more realistic than the one by weak perspective projection in Fig. 5(b).

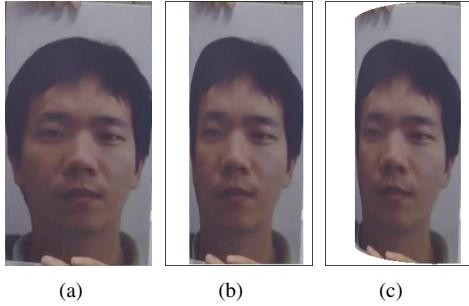


Figure 5: Different projections. (a) Texture of the cropped printed photo region. (b) Rendered texture by weak perspective projection. (c) Rendered texture by perspective projection.

3.3. Post-processing

Due to the mesh deformation and perspective projection, the size of synthetic photos will be changed (see Fig. 6(a)).

To improve the fidelity of the final synthetic sample, we try to make sure the synthetic printed photo fully overlaps the originally printed photo region (see Fig. 6). Besides, the gaussian image filter is applied to make the fused edge smoother. Several final synthetic spoof results are shown in Fig. 1.

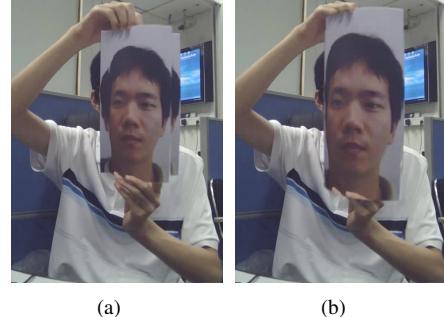


Figure 6: Post-processing of the synthetic printed photo. (a) Fused image without full overlapping. (b) Fused image with full overlapping.

4. Deep Network Training on Synthetic Data

In this section, we present our approach to training from synthetic spoof data. Fig. 7 shows a high-level illustration of our training pipeline. Virtual synthetic spoof samples are used to supervise the network training with our data balancing methods.

Data Balancing. We can generate as many spoof samples as we want by the synthesis method, but the amount of live samples is fixed. As a result, the CNN model trained has a bias to virtual spoofs due to the imbalance of live and virtual spoof samples.

There are two methods to mitigate the impact of data imbalance: balanced sampling strategy and importing external live samples. To perform balanced sampling, the ratio of sampled live and spoof instances in each min-batch is kept fixed during training after augmenting dataset. Besides, the live samples are much easier to acquire than the spoof ones in practical applications, such as the samples from face recognition databases [12, 16]. Therefore, unlimited external live samples can be imported to balance the distribution of training data.

How to Treat Synthetic Samples. The previous synthesis-based work [4] first uses the synthetic samples to train one initialization model and then fine-tunes it on the real data. Since our synthesis is high-fidelity and possesses much more variations than the real data, we treat equally the synthetic spoof samples with the real ones and directly train models on the joint data of synthetic and real data.

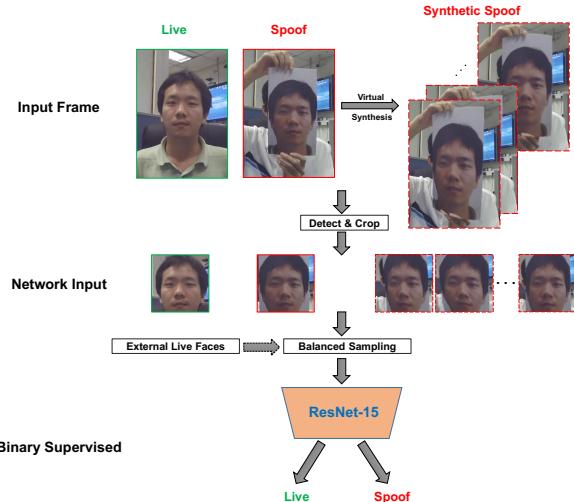


Figure 7: The pipeline of our proposed deep network training with synthetic data.

5. Experiments

We evaluate the effectiveness of learning with virtual synthetic data from two aspects: CASIA-MFSD [40] and Replay-Attack [5] for intra-database evaluation and CASIA-RFS [18] for inter-database evaluation. Performance evaluations on CASIA-MFSD and Replay-Attack databases are for fair comparisons with other previous methods. The CASIA-RFS database is much more challenging since it contains rotated live and spoof faces with various poses. We use it as the testing set and the entire CASIA-MFSD database as the training set to carry out the inter-database testing.

5.1. Database and Protocols

CASIA-MFSD. This database contains 50 subjects, and 12 videos for each subject under different resolutions and light conditions. Three different spoof attacks are designed: replay, warp print and cut print attacks. The database contains 600 video recordings, in which 240 videos of 20 subjects are used for training and 360 videos of 30 subjects for testing.

Replay-Attack. This database consists of 1,300 videos from 50 subjects. These videos are collected under controlled and adverse conditions and are divided into training, development and testing sets with 15, 15 and 20 subjects respectively.

CASIA-RFS. This database contains 785 videos for genuine faces and 1950 videos for spoof faces. The videos are collected using three devices with different resolutions: Digital camera (DC), mobile phone (MP) and web camera (WC). Two kinds of spoof attacks including planar and bent photo attacks are designed.

Protocols. For CASIA-MFSD and Replay-Attack databases, our experiments follow the associated protocols,

Table 1: Our ResNet-15 network structure. Conv3.x, Conv4.x, and Conv5.x indicate convolution units which may contain multiple convolution layers, and residual blocks are shown in double-column brackets. e.g. $[3 \times 3, 128] \times 3$ denotes 3 cascaded convolution layers 128 feature maps with filters of size 3×3 , and S2 denotes stride 2.

Layers	15-layer CNN	
Conv1.x	$[5 \times 5, 32] \times 1$, S2	
Conv2.x	$[3 \times 3, 64] \times 1$, S1	
Conv3.x	$[3 \times 3, 128]$ $[3 \times 3, 128]$	$\times 2$, S2
Conv4.x	$[3 \times 3, 256]$ $[3 \times 3, 226]$	$\times 2$, S2
Conv5.x	$[3 \times 3, 512]$ $[3 \times 3, 512]$	$\times 2$, S2
Global Pooling & FC	512	

the EER and HTER indicators are reported. The Replay-Attack database has already provided a development set thus our HTER threshold is determined on it. As for inter-database evaluation, we build the protocols following [43]. Attack Presentation Classification Error Rate (APCER), Bona Fide Presentation Classification Error Rate (BPCER), Average Classification Error Rate (ACER), Top-1 accuracy are all evaluated. Particularly, the APCER here represents the highest error among plane printed and bending printed attacks.

5.2. Implementation Details

Network Structure. Our network structure is based on ResNet [14]. The input size of original ResNet is 224×224 , while ours is 120×120 . Therefore, the original 7×7 convolution in the first layer is replaced by 5×5 and follows one 3×3 convolution layer to preserve the dimension of feature map output. Finally, one 15 layers ResNet (ResNet-15) structure is designed for our task and shown in Table 1.

Training. Our experiments are based on PyTorch framework and GeForce GTX TITAN X GPU devices. All training images are cropped and aligned to size 120×120 by similar transformation, then being normalized by subtracting 127.5 and being divided by 128. For all three databases, we use SGD with a mini-batch size of 64 to optimize the network, with the weight decay of 0.0005 and momentum of 0.9. Image horizontal flipping is adopted as standard augmentation. The weight parameters of ResNet-15 model are randomly initialized. We train 30 epochs for each experiment. We set the initial learning rate of 0.1, then decrease it by multiplying 0.1 in 10th and 20th epoch respectively.

The ratios of the number of live/spoof samples on the CASIA-MFSD and Replay-Attack databases are all about 1:3, we keep this ratio in each mini-batch sampling on

Table 2: ACER(%), Top-1(%), EER(%) and HTER(%) on CASIA-MFSD with different projections.

Projection	ACER (%)	Top-1 (%)	EER (%)	HTER (%)
Weak Perspective	3.33	97.78	2.59	2.41
Perspective	2.22	98.61	2.22	1.67

Table 3: ACER(%), Top-1(%), EER(%) and HTER(%) on CASIA-FASD for inter-database testing with different learning methods. BS indicates the balanced sampling strategy.

Method	ACER (%)	Top-1 (%)	EER (%)	HTER (%)
Baseline (I-A)	5	96.67	4.44	3.89
Synthesis w/o BS (I-B)	4.44	97.78	3.33	2.78
Synthesis w/ BS (I-C)	2.22	98.61	2.22	1.67

augmented training data when applying balanced sampling. More comparisons can be referred to Sec.5.3. For inter-database testing in Sec.5.3.3, we use part of CMU MultiPIE Face Database (MultiPIE) [12]. Totally, 8,120 face images with various poses are introduced as external data.

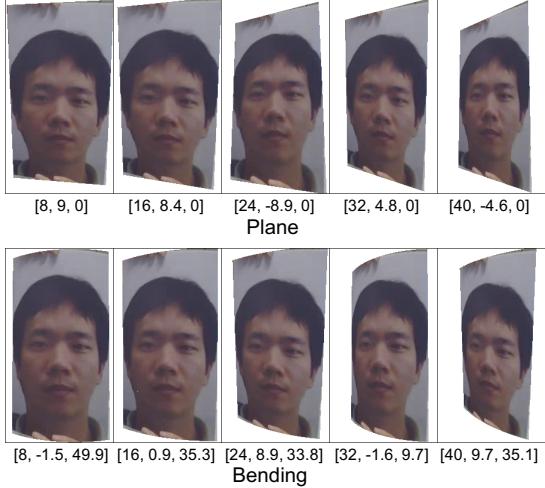


Figure 8: Synthetic samples before post-processing. The first row: five synthesized planar samples. The second row: five synthesized vertically bent samples. The values in brackets indicate yaw, pitch, and bending angle successively.

Synthesis. For each printed spoof instance in CASIA-MFSD and Replay-Attack, we generate ten synthetic samples, in which five samples are rotated and bent, another five ones are only rotated. For each replay spoof sample, we generate five synthetic samples without bending, since the replay devices cannot be bent. During rotating, the yaw angle is uniformly drawn from the interval [0, 40], the pitch angle is from [-10, 10] and the bending angle is from [30, 60]. We show one example in Fig. 8.

Table 4: ACER(%), Top-1(%), EER(%) and HTER(%) on Replay-Attack with different learning methods. BS indicates the balanced sampling.

Method	ACER (%)	Top-1 (%)	EER (%)	HTER (%)
Baseline (II-A)	4.17	98.13	2.50	3.50
Synthesis w/o BS (II-B)	2.50	98.14	1.25	1.75
Synthesis w/ BS (II-C)	0.21	99.79	0.25	0.63

Table 5: APCERs (%) and BPCER (%) on CASIA-MFSD and Replay-Attack with different learning methods.

Database	Method	APCER (Replay, %)	APCER (Print, %)	BPCER (%)
CASIA-MFSD	Baseline (I-A)	3.33	1.67	6.67
	Synthesis w/BS (I-C)	2.22	0.56	1.67
Replay-Attack	Baseline (II-A)	0.63	0.83	7.5
	Synthesis w/BS (II-C)	0	0.42	0

Table 6: APCER(%), BPCER(%), ACER (%) and Top-1(%) on CASIA-RFS with different learning methods.

Method	APCER (%)	BPCER (%)	ACER (%)	Top-1 (%)
Baseline (III-A)	20.96	23.98	22.47	81.83
Synthesis w/o MultiPIE (III-B)	4.01	50.23	27.12	82.63
Synthesis w/ MultiPIE (III-C)	4.68	18.75	11.72	91.68

5.3. Experimental Comparison

5.3.1 Ablation Study

We evaluate the performances of different strategies of projections, synthetic data, and data balancing in this section.

Projection. We explore weak perspective and perspective projections of spoof data synthesis. From results in Table 2, we can see that the perspective projection has a significant improvement compared with the weak perspective projection with an EER 2.22% and an HTER 1.67%. Moreover, ACER improves from 3.33% to 2.22% and Top-1 accuracy rises from 97.78% to 98.61%. The results indicate that perspective projection is more suitable for virtual spoof data synthesis.

Synthetic Data & Balanced Sampling (BS). For CASIA-MFSD and Replay-Attack in Table 3 and Table 4, we compare three options: (A) The original dataset is used without the synthetic spoof data and BS. (B) The synthetic spoof data is applied. (C) Both the synthetic data and BS are adopted. We can observe that I-B (II-B) is considerably better than I-A (II-A) in ACER, Top-1 accuracy, EER, and HTER. This result shows the synthetic spoof data is effective for training CNN. Also, both I-C and II-C achieve the best performances, which verifies the effectiveness of our BS. Besides, the combination of synthetic samples and BS can further promote the performance.

Moreover, we evaluate APCER under replay and print attacks and BPCER in Table 5. The results show that APCER improves under both attacks on CASIA-MFSD and Replay-Attack. It indicates that the classification accuracies of spoof samples become better, which we attribute to virtual

Table 7: EER (%) and HTER (%) on CASIA-FASD. BS indicates the balanced sampling strategy.

Method	EER (%)	HTER (%)
Fine-tuned VGG-Face [19]	5.20	-
DPCNN [19]	4.50	-
Multi-Scale [38]	4.92	-
CNN [37]	6.20	7.34
LSTM-CNN [37]	5.17	5.93
YCbCr+HSV-LBP [2]	6.20	-
Feature Fusion [33]	3.14	-
Fisher Vector [3]	2.80	-
Patch-based CNN [1]	4.44	3.78
Depth-based CNN [1]	3.78	2.52
Patch&Depth Fusion [1]	2.67	2.27
Ours (Synthesis w/BS)	2.22	1.67

Table 8: EER (%) and HTER (%) on Replay-Attack. BS indicates the balanced sampling strategy.

Method	EER (%)	HTER (%)
Fine-tuned VGG-Face [19]	8.40	4.30
DPCNN [19]	2.90	6.10
Multi-Scale [38]	2.14	-
YCbCr+HSV-LBP [2]	0.40	2.90
Fisher Vector [3]	0.10	2.20
Moire pattern [27]	-	3.30
Patch-based CNN [1]	4.44	3.78
Depth-based CNN [1]	3.78	2.52
Patch&Depth Fusion [1]	0.79	0.72
FASNet [22]	-	1.20
Ours (Synthesis w/BS)	0.25	0.63

synthetic data. In addition, the BPCER gets better, and we think it is because of BS.

External Live Samples. For CASIA-RFS in Table 6, we compare three options: (A) Neither synthetic data or MultiPIE is used. (B) The synthetic spoof data is used. (C) Both MultiPIE and the synthetic spoof data are used. In both III-B and III-C, balanced sampling is applied. Compared to the baseline, the join of synthetic data makes APCER decrease from 20.96% in III-A to 4.01% in III-B, but BPCER in III-B becomes higher than III-A. It shows that the spoof data classification accuracy improves while the live face classification precision drops. We think that it is because live faces in CASIA-RFS have a wide range of poses, while the range of faces posture in CASIA-MFSD is limited. Once MultiPIE is used in III-C to balance the training data, BPCER drops obviously from 50.23% in III-B to 18.75% in III-C. Besides, APCER remains almost unchanged from III-B to III-C. Finally, the Top-1 and EER indicators on CASIA-RFS get improved by 9.85% and 9.67% respectively from III-A to III-C. The above results show that external live data, *e.g.* MultiPIE, can improve the generalization by a large margin.

Table 9: APCER (%), BPCER (%), ACER(%) and Top-1(%) on CASIA-RFS for inter-database testing.

Method	APCER (%)	BPCER (%)	ACER (%)	Top-1 (%)
FASNet [22]	1.23	47.27	24.25	84.48
Patch-based CNN [1]	12.93	29.89	21.41	83.54
Baseline (III-A)	20.96	23.98	22.47	81.83
Ours	4.68	18.75	11.72	91.68

5.3.2 Intra-database Testing

The intra-database testing is performed on the CASIA-MFSD and Replay-Attack databases. Table 7 shows the comparisons of our proposed synthesis-based method with the state-of-the-art methods. Among these methods in Table 7, the CNN in [19, 39, 19] is used as the feature extractor, and the SVM or softmax classifier is used for live/spoof classification. The work in [1] performs binary classification through utilizing local features from patch inputs and holistic features by regressing pseudo-depth. As shown in Table 7, our synthesis-based method outperforms other methods in both EER and HTER.

For Replay-Attack database, we evaluate our method with other methods in Table 8. We can see the proposed method also outperforms other state-of-the-art methods. Though our method has similar EER with several methods, the HTER is smaller than theirs, which means we have lower false acceptance and true rejection rates.

5.3.3 Inter-database Testing

We perform the inter-database testing on CASIA-RFS, in which CASIA-MFSD is used as the training set. In Table 9, we compare our method with other CNN-based methods and our baseline. The other CNN-based methods are re-implemented following the descriptions in original papers. The results show that the proposed method outperforms other CNN-based methods and our baseline in generalization. The inter-database testing also verifies the effectiveness of synthetic spoof data and the data balancing strategy.

6. Conclusion

In this paper, we have shown successful large-scale training of CNNs from synthetically generated spoof data. For the data imbalance brought by spoof data, we exploit two methods for balancing it: balanced sampling and adding external live samples. Our synthetic spoof data and data balancing methods greatly promote the performance for face anti-spoofing. The results show the great potential for advancing face anti-spoofing using large-scale synthetic data. Besides, more realistic and more kinds of spoof synthesis are future directions.

References

- [1] Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu. Face anti-spoofing using patch and depth-based cnns. In *IJCB*, 2017. 1, 2, 7
- [2] Z. Boulkenafet, J. Komulainen, and A. Hadid. Face anti-spoofing based on color texture analysis. In *ICIP*, 2015. 7
- [3] Z. Boulkenafet, J. Komulainen, and A. Hadid. Face anti-spoofing using speeded-up robust features and fisher vector encoding. *IEEE Signal Processing Letters*, 2017. 7
- [4] W. Chen, H. Wang, Y. Li, H. Su, Z. Wang, C. Tu, D. Lischinski, D. Cohen-Or, and B. Chen. Synthesizing training images for boosting human 3d pose estimation. In *3DV*, 2016. 2, 4
- [5] I. Chingovska, A. Anjos, and S. Marcel. On the effectiveness of local binary patterns in face anti-spoofing. In *BIOSIG*, 2012. 2, 5
- [6] T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel. Lbp-top based countermeasure against face spoofing attacks. In *ACCV*, 2012. 1
- [7] T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel. Can face anti-spoofing countermeasures work in a real world scenario? In *ICB*, 2013. 1
- [8] Y. Du, Y. Wong, Y. Liu, F. Han, Y. Gui, Z. Wang, M. Kankanhalli, and W. Geng. Marker-less 3d human motion capture with monocular image sequence and height-maps. In *ECCV*, 2016. 2
- [9] L. Feng, L. Po, Y. Li, X. Xu, F. Yuan, T. C. Cheung, and K. Cheung. Integration of image quality and motion cues for face anti-spoofing: A neural network approach. *Journal of Visual Communication and Image Representation*, 2016. 2
- [10] J. Gan, S. Li, Y. Zhai, and C. Liu. 3d convolutional neural network based on face anti-spoofing. In *ICMIP*, 2017. 2
- [11] M. F. Ghezelghieh, R. Kasturi, and S. Sarkar. Learning camera viewpoint using cnn to improve 3d body pose estimation. In *3DV*, 2016. 2
- [12] R. Gross, I. Matthews, J. Cohn, T. Kanade, and S. Baker. Multi-pie. *Image and Vision Computing*, 2010. 4, 6
- [13] J. Guo, X. Zhu, Z. Lei, and S. Z. Li. Face synthesis for eyeglass-robust face recognition. *arXiv:1806.01196*, 2018. 2, 3, 4
- [14] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. In *CVPR*, 2016. 5
- [15] G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller. Labeled faces in the wild: A database forstudying face recognition in unconstrained environments. In *Workshop on faces in 'Real-Life' Images: detection, alignment, and recognition*, 2008. 1
- [16] I. Kemelmacher-Shlizerman, S. M. Seitz, D. Miller, and E. Brossard. The megaface benchmark: 1 million faces for recognition at scale. In *ICCV*, 2016. 1, 4
- [17] J. Komulainen, A. Hadid, and M. Pietikainen. Context based face anti-spoofing. In *BTAS*, 2013. 1
- [18] Z. Lei, W. Tao, X. Zhu, T. Fu, and S. Z. Li. Countermeasures to face photo spoofing attacks by exploiting structure and texture information from rotated face sequences. *Mobile Biometrics*, 2017. 2, 5
- [19] L. Li, X. Feng, Z. Boulkenafet, Z. Xia, M. Li, and A. Hadid. An original face anti-spoofing approach using partial convolutional neural network. In *IPTA*, 2016. 1, 2, 7
- [20] J. Liebelt and C. Schmid. Multi-view object class detection with a 3d geometric model. In *CVPR*, 2010. 2
- [21] Y. Liu, A. Jourabloo, and X. Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In *CVPR*, 2018. 1, 2
- [22] O. Lucena, A. Junior, V. Moia, R. Souza, E. Valle, and R. Lotufo. Transfer learning using convolutional neural networks for face anti-spoofing. In *ICCIAR*, 2017. 7
- [23] F. Massa, B. C. Russell, and M. Aubry. Deep exemplar 2d-3d detection by adapting from real to rendered views. In *CVPR*, 2016. 2
- [24] C. Nagpal and S. R. Dubey. A performance evaluation of convolutional neural networks for face anti spoofing. *arXiv:1805.04176*, 2018. 2
- [25] G. Pan, L. Sun, Z. Wu, and S. Lao. Eyeblink-based anti-spoofing in face recognition from a generic webcam. 2007. 1
- [26] K. Patel, H. Han, and A. K. Jain. Cross-database face anti-spoofing with robust feature representation. In *CCBR*, 2016. 1, 2
- [27] K. Patel, H. Han, A. K. Jain, and G. Ott. Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In *ICB*, 2015. 7
- [28] L. Pishchulin, A. Jain, M. Andriluka, T. Thormählen, and B. Schiele. Learning people detection models from few training samples. In *CVPR*, 2011. 2, 3
- [29] L. Pishchulin, A. Jain, M. Andriluka, T. Thormählen, and B. Schiele. Articulated people detection and pose estimation: Reshaping the future. In *CVPR*, 2012. 2, 3
- [30] H. Rahmani and A. Mian. Learning a non-linear knowledge transfer model for cross-view action recognition. In *CVPR*, 2015. 2, 3
- [31] H. Rahmani and A. Mian. 3d action recognition from novel viewpoints. In *CVPR*, 2016. 2
- [32] G. Rogez and C. Schmid. Mocap-guided data augmentation for 3d pose estimation in the wild. In *NIPS*, 2016. 2
- [33] T. A. Siddiqui, S. Bharadwaj, T. D. I, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha. Face anti-spoofing with multifeature videolet aggregation. In *ICPR*, 2016. 7
- [34] H. Su, C. R. Qi, Y. Li, and L. J. Guibas. Render for cnn: Viewpoint estimation in images using cnns trained with rendered 3d model views. In *ICCV*, 2015. 2
- [35] Z. Wang, C. Zhao, Y. Qin, Q. Zhou, and Z. Lei. Exploiting temporal and depth information for multi-frame face anti-spoofing. *arXiv:1811.05118*, 2018. 2
- [36] L. Wolf, T. Hassner, and I. Maoz. Face recognition in unconstrained videos with matched background similarity. In *CVPR*, 2011. 1
- [37] Z. Xu, S. Li, and W. Deng. Learning temporal features using lstm-cnn architecture for face anti-spoofing. In *ACPR*, 2015. 1, 2, 7
- [38] J. Yang, Z. Lei, and S. Z. Li. Learn convolutional neural network for face anti-spoofing. *arXiv:1408.5601*, 2014. 2, 7

- [39] J. Yang, Z. Lei, S. Liao, and S. Z. Li. Face liveness detection with component dependent descriptor. *ICB*, 2013. [1](#), [7](#)
- [40] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li. A face antispoofing database with diverse attacks. In *ICB*, 2012. [2](#), [5](#)
- [41] X. Zhu, Z. Lei, X. Liu, S. Z. Li, et al. Face alignment in full pose range: A 3d total solution. *TPAMI*, 2017. [2](#), [4](#)
- [42] X. Zhu, Z. Lei, X. Liu, H. Shi, and S. Z. Li. Face alignment across large poses: A 3d solution. In *CVPR*, 2016. [2](#)
- [43] B. Zinelabidine, K. Jukka, L. Li, X. Feng, and A. Hadid. Oulunpu: a mobile face presentation attack database with real-world variations. In *ISBA*, 2017. [5](#)