Multi-Perspective Features Learning for Face Anti-Spoofing

Zhuming Wang¹, Yaowen Xu¹, Lifang Wu∗¹,², Hu Han³, Yukun Ma⁴, and Guozhang Ma¹

¹Beijing University of Technology, Beijing 100124, China
²Beijing Key Laboratory of Computational Intelligence and Intelligent System
³Key Laboratory of Intelligent Information Processing of Chinese Academy of Sciences (CAS), Institute of Computing Technology, CAS, Beijing 100190, China
⁴Henan Institute of Science and Technology, Henan, China

Abstract

Face anti-spoofing (FAS) is important to securing face recognition. Most of the existing methods regard FAS as a binary classification problem between bona fide (real) and spoof images, training their models from only the perspective of Real vs. Spoof. It is not beneficial for a comprehensive description of real samples and leads to degraded performance after extending attack types. In fact, the spoofing clues in various attacks can be significantly different. Furthermore, some attacks have characteristics similar to the real faces but different from other attacks. For example, both real faces and video attacks have dynamic features, and both mask attacks and real faces have depth features. In this paper, a Multi-Perspective Feature Learning Network (MPFLN) is proposed to extract representative features from the perspectives of Real + Mask vs. Photo + Video and Real + Video vs. Photo + Mask. And using these features, a binary classification network is designed to perform FAS. Experimental results show that the proposed method can effectively alleviate the above issue of the decline in the discrimination of extracted features and achieve comparable performance with state-of-the-art methods.

1. Introduction

In recent years, with the wide application of face recognition technology [10] in identity authentication systems, such as financial payment and access control unlock, the attempts of presentation attacks (PAs) against it are also increasing. Using PAs like photo-print, video-replay, and 3D masks [11], attackers can deceive the face recognition system easily, thus posing a severe threat to users’ private property and even the public security of society. Therefore, it is needed to develop an effective face anti-spoofing (FAS) method.

Presentation attack detection (PAD) has been studied for over a decade. In the early days, researchers attempted to use human liveness cues [13, 21, 17] or handcrafted texture features [3, 6, 5, 15, 22, 27] to perform binary classification on bona fide (real) and spoof faces. Recently, with the rapid development of deep learning technology, convolutional neural networks (CNN) based methods [7, 16, 34, 18, 32] have shown significant performance improvement compared with traditional methods. Feng et al. [7], Li et al. [16] trained a deep neural network to learn real/spoof faces classification. Face depth map and rPPG signal were utilized in [18] as the auxiliary supervision to train the proposed model. A well-designed Central Difference Convolutional Network (CDCN) was used in [34] to extract face depth information for PAD which achieved competitive performance.

However, most existing methods considered FAS as a binary classification problem between real faces and spoof faces, ignoring the differences between different attack types and their commonness with real faces. Although some methods utilize auxiliary information as supervision, their perspective of group-level classification is still Real vs. Spoof in the training stage. It is feasible when there are only photo-print and video replay attacks due to their similar spoofing clues. However, when the 3D mask attack is considered, the limitation of binary classification is distinctly presented because 3D masks have quite different spoofing clues from photo and video attacks.

In fact, different attack types present different spoofing features, and spoofing features that can detect one particular attack type well (features this type of attack has while real faces do not) may not exist in another attack type, and trying to find some universal features that can detect multiple...
attack types possibly is a tradeoff of different attacks, which may not be optimal to each attack type. On the other hand, considered from different perspectives, there are common features between the attack types and real faces. For example, as shown in Fig.1, both real faces and 3D masks have depth information while photos and videos do not; both real faces and videos have dynamic information while photos and 3D masks do not. Therefore, by selecting appropriate perspectives, it is possible to obtain a more comprehensive description of real faces and avoid the network neglecting some features that have a strong discriminating ability between real and spoof faces yet are not universal among a variety of attack types, thus improve the performance of FAS.

Motivated by the discussions above, we propose a Multi-Perspective Features Learning strategy to extract more comprehensive description to real faces using a Real + 1 vs. Rest group-level classification training strategy, i.e., images of real faces and a given attack type are used as positive samples, and images of the rest of the attack types are used as negative samples for group-level classification. Furthermore, considering the wide application of depth and temporal information in PAD, two perspectives of Real + Mask vs. Rest and Real + Video vs. Rest are selected, and a novel Multi-Perspective Features Learning Network (MPFLN) is designed to extract the common features between real faces and video or mask attacks for FAS. The proposed network consists of two components: the Common Features Extraction Unit (CFEU) to extract the representative features and the Binary Classification Unit (BCU) that utilizes common features to classify real and spoof faces.

The main contributions of this work can be summarized as follows:

- We find the limitation of binary classification to FAS and propose a novel idea of Multi-Perspective Feature Learning, which can extract the features of real faces more comprehensively. These features have a strong discriminating ability between real and spoof faces yet are not universal among a variety of attack types.
- A novel neural network called Multi-Perspective Features Learning Network (MPFLN) is designed, which can simultaneously detect multiple types of attacks, including photos, videos, and masks, and effectively carry out the FAS task.
- The proposed MPFLN achieves competitive performance in the test database. Well-designed comparative experiments demonstrate the negative impact on the model’s classification performance of retraining with the introduction of new attack types and the effectiveness of the method of Multi-Perspective Feature Learning to alleviate this problem.

2. Related work

Traditional approaches. Traditional methods usually focus on the texture difference between real and spoof faces brought by spoof media, using handcrafted features extracted from images, such as LBP [3, 5], HOG [15], SIFT [22], and DoG [27], to carry out binary classification of real and spoof faces. However, these features are usually based on 2D features, such as the noise brought by printing paper or video replay equipment, which is difficult to be applied on the 3D mask attacks. Similarly, the texture features extracted for masks [23, 1] are also difficult to be applied to the detection of photos and videos. There are also several methods considering temporal information and using dynamic texture [14, 28] or spontaneous human movement [13, 21] like blinking and head motion to perform PAD. These methods have achieved good performance in detecting photos and
static videos, and mask attack detection methods using dynamic information \cite{24,25} also have certain effects. Still, these methods are difficult to detect attacks that naturally contain dynamic information such as video replay.

**Deep learning approaches.** With the rapid development of deep learning, some deep learning based approaches were proposed. Feng et al. \cite{7}, Li et al. \cite{16} using pre-trained CNN as a feature extractor to distinguish real and spoofing faces. Xu et al. \cite{31} using LSTM architecture to combine spatial information with temporal information for attack detection. In addition to methods considering FAS as a simple binary classification problem supervised by the binary cross-entropy loss, some works using pseudo depth label \cite{2,35}, rPPG signal \cite{20}, binary mask label \cite{9,26,19}, Fourier map \cite{12}, LBP texture Map \cite{35}, etc., as auxiliary supervision, have also achieved good performance. Liu et al. \cite{18} introduced face depth map and rPPG signal as auxiliary supervision guiding feature extraction. Yu et al. \cite{34} using a well-designed Central Difference Convolutional Network (CDCN) to extract face depth information for PAD and achieved good performance.

However, most existing work only focuses on dealing with photo and video attacks and has difficulty covering mask attacks. Also, approaches aimed to mask attacks can not deal well with the former attacks either. The reason is that the differences between them are so significant that it’s hard to find some universal clues which can identify multiple attacks at the same time. Trying to find such clues can lead to a decline in the discrimination on spoofing features of each attack type. Therefore, we use a Multi-Perspective Feature Learning method to retain clues that have a strong discriminating ability for each attack type, thus preventing a decrease in the discrimination on features.

**3. Methodology**

The main idea of the proposed method is to extract the representative features from multiple perspectives to describe real faces more discriminatively. As shown in Fig.2, the proposed network consists of two modules: Common Features Extraction Unit (CFEU) and Binary Classification Unit (BCU). For the convenience of description, we only take common attacks, including photo-print, video-replay, and 3D mask as examples, to introduce the proposed network in this paper.

**3.1. Common Features Extraction Unit**

The Common Features Extraction Unit is used to extract the common features with strong discrimination between real faces and various attack types from multiple perspectives. Therefore, unlike the traditional binary classification, CFEU uses the perspective of Real + 1 vs. Rest instead of Real vs. Spoof for group-level classification training. In addition, considering the wide application of depth information and timing information in PAD, we only build two parts in CFEU: Real_Mask part (RM) and Real_Video part (RV), which are beneficial to the extraction of depth and temporal information, respectively, but not the Real_Photo part whose features are not prominently.

**Real_Mask part.** The function of RM is to extract the common features with strong discrimination between real faces and mask attacks. For this purpose, we adopt the Real + Mask vs. Rest group-level classification training strategy. Specifically, let $I_R, I_P, I_S, I_M$ denote the set of the real face images, photo attack images, video attack images, and mask attack images in the whole sample space respectively. For any input image $X \in I$, we use PRNet \cite{8} to generate its pseudo depth map $D \in \mathbb{R}^{d \times d}$, and its corresponding group-
level classification label $Y_{rm}$ can be formulated as

$$Y_{rm} = \begin{cases} D, & X \in (I_R \cup I^m_S) \\ Z, & X \in (I^p_S \cup I^v_S) \end{cases},$$

(1)

where $Z \in \mathbb{R}^{d \times d}$ is a ‘zero map’ with the same shape as $D$.

Then, we extract the feature map $P_{rm} = E_{rm}(X)$ as the predicted depth map of $X$ by RM Features Extractor ($E_{rm}$), and $Y_{rm}$ is used as the supervision to train the extraction capacity of group-level classification features (the common features between Real and Mask) of $E_{rm}$. Here, $E_{rm}$ uses the famous CDCN [34] as the backbone network. Therefore, the loss function of RM can be formulated as

$$L_{rm} = \sum_{i=1}^{N} L_{MSE}(P^i_{rm}, Y^i_{rm}) + L_{CDL}(P^i_{rm}, Y^i_{rm}),$$

(2)

where $N$ is the total samples number of the training set, $L_{MSE}$ and $L_{CDL}$ denote mean square error loss and contrastive depth loss [29], respectively. Notice that, although the network structure and the loss function of RM are basically the same as the backbone network, the meaning of RM’s group-level classification label (Real + Mask vs. Rest) has a completely different meaning than the traditional one (Real vs. Spoof).

**Real/Video part.** Similar to RM, RV is used to extract the common features with strong discrimination between real faces and video attacks by adopting a Real + Video vs. Rest group-level classification training strategy. Since CDCN is mainly used to extract depth information but is not good at extracting temporal information, we use 3D-CDCN [30], a variant of CDCN, as the backbone network of $E_{rv}$. Compared with CDCN, 3D-CDCN can extract the temporal information of input frame sequences, which is more suitable for the group-level classification criterion of RV.

Therefore, the process of RV is modified as: for any input frame sequence $X \in I$, we extract the feature map $P_{rv} = E_{rv}(X)$ of $X$ by RV Features Extractor ($E_{rv}$) and use $Y_{rv}$ as the supervision to train the extraction capacity of group-level classification features (the common features between Real and Video) of $E_{rv}$. Consistent with 3D-CDCN, the corresponding group-level classification label $Y_{rv}$ of $X$ can be formulated as

$$Y_{rv} = \begin{cases} O, & X \in I_R \\ Z, & X \in (I^p_S \cup I^v_S \cup I^m_S) \end{cases},$$

(3)

where $O \in \mathbb{R}^{d \times d}$ is a ‘one map’ with the same shape as $Z$.

The loss function of RV can be formulated as

$$L_{rv} = \sum_{i=1}^{N} L_{MSE}(P^i_{rv}, Y^i_{rv}),$$

(4)

where $\{P^i_{rv}, Y^i_{rv}\}$ are the fusion network $F$ consisting of three convolution layers and get the output $P_f = F(P_{rv}, Y_{rv})$. The corresponding real/spoof classification label $Y_f$ of $X$ can be formulated as

$$Y_f = \begin{cases} O, & X \in I_R \\ Z, & X \in (I^p_S \cup I^v_S \cup I^m_S) \end{cases},$$

(5)

The loss function of BCU module formulated as

$$L_f = \sum_{i=1}^{N} L_{MSE}(P^i_f, Y^i_f),$$

(6)

In the testing stage, we calculate the mean value of $P_f$ as the final score of the real/spoof binary classification task.

3.2. Binary Classification Unit

BCU is used to classify the real faces and the spoof attacks through the $E_{rm}$ and $E_{rv}$ obtained from CFEU. Specifically, for any input $X$, we concatenate its corresponding $P_{rm}$, $P_{rv}$ obtained from CFEU, then fed them into the fusion network $F$ consisting of three convolution layers and get the output $P_f = F(P_{rm}, P_{rv})$. The corresponding real/spoof classification label $Y_f$ of $X$ can be formulated as

$$Y_f = \begin{cases} O, & X \in I_R \\ Z, & X \in (I^p_S \cup I^v_S \cup I^m_S) \end{cases},$$

The loss function of BCU module formulated as

$$L_f = \sum_{i=1}^{N} L_{MSE}(P^i_f, Y^i_f),$$

In the testing stage, we calculate the mean value of $P_f$ as the final score of the real/spoof binary classification task.

Notice that, we suggest that CFEU and BCU should be trained in two-stage rather than end-to-end format, i.e., the CFEU part should be trained first, and its parameters should be fixed during training the BCU part. The reason is that the classification labels of RM, RV conflict with F, thus optimizing F leads to an offset towards the corresponding negative samples of the mask class in RM and the video class in RV, which is contrary to the motivation of our proposed method.

4119
4. Experiments

4.1. Datasets and Protocols

**Databases.** Two datasets, including OULU-NPU [4] and CASIA-SURF 3DMask [33], are used in our experiments. Oulu-NPU contains high-resolution attack samples of photo-prints and video-replays, but does not contain 3D mask attack samples. To this end, we introduce the mask attack samples from CASIA-SURF 3DMask as a supplementary set to the former dataset.

**Protocols.** Based on the four test protocols of OULU-NPU, we extend the attack type of the 3D mask and design two sets of experiments. In the first set, we only expanded the training set by mask samples with the same number of photos and videos, while the validation set and testing set remained unchanged. This set of experiments is named Experiment-O, which is used to prove that our method can achieve comparable performance with state-of-the-art methods. In the second set, we expanded mask samples in not only the training set but the validation set and the testing set also. This set of experiments is named Experiment-M, which is used to prove that, by extracting representative features from multiple perspectives, the decline in the discrimination after extending attack types suffered by existing methods can be alleviated effectively.

**Performance Metrics.** We adopt Attack Presentation Classification Error Rate (APCER), Bona Fide Presentation Classification Error Rate (BPCER), and Average Classification Error Rate (ACER) as the performance metrics.

4.2. Implementation Details

**Ground Truth Generation.** Although MPFLN adopts the fully convolutional structure and has no requirements on the size of input images, for the convenience of analysis, we detect the face regions of input images then crop and resize their scales to $256 \times 256$. Consistent with CDCN, we adopt PRNet [8] to generate pseudo depth maps of images, resize their scales to $32 \times 32$, and normalized them to $[0, 1]$. Accordingly, the scales of all the $1/0$ maps used in the model are also $32 \times 32$. Input images and their corresponding pseudo depth maps and $1/0$ maps are shown in Fig.3.

**Experimental Setting.** Our proposed method is implemented with Pytorch. In the training stage, RM, RV, and BCU are trained with Adam optimizer, and the initial learning rate (lr) is 1e-4, 1e-3, and 5e-4, respectively, and weight decay (wd) is 1e-5. We train RM, RV with a maximum of 600 epochs while lr halves every 300 epochs and set 500/200 for BCU. The batch size is 16.

4.3. Experimental Comparison

**Experiment-O.** Since most of the comparison methods only used photo and video attacks in training, although MPFLN has the ability to detect mask attacks, we still only considered the photo and video attacks in this set of experiments. In other words, mask samples were only introduced in the training stage of MPFLN, while the testing stage was consistent with the comparison experiments, using OULU-NPU samples only and following its four protocols. Notice that, although mask samples are introduced into the training set, they are not conducive to be used as expanded data to enhance the discrimination of the other two attack types due to the significant difference between them. On the contrary, this large difference leads to a deviation of the feature extraction direction of the model after introducing mask attack samples in training, which eventually raises the risk of the decrease of the model’s overall performance.

As shown in Table 1, our method can achieve comparable performance with the state-of-the-art methods on most protocols, only has a decline in the performance on protocol 4. It means that, although our method can alleviate the decline of feature discrimination caused by introducing mask attack samples in most conditions, it is still impacted severely on protocol 4. The reason for this is, while
experiment-M. In structure, MPFLN can easily be confused with the Model Stacking strategy. However, the two are fundamentally different in method. The purpose of MPFLN is to extract the representative features from multiple perspectives for classification. Hence the label of CFEU is in Real + 1 vs. Rest form, rather than the traditional Real vs. Spoof form. To demonstrate that the performance improvement of MPFLN is due to the group level classification strategy rather than the Model Stacking strategy, we design this set of experiments. We compare the performance of three models: CDCN-rs, whose structure is identical to CDCN, but is retrained after introducing mask attacks in the negative sample; MPFLN-rs, whose structure is identical to MPFLN, but the CFEU module classify the samples by Real vs. Spoof perspective; MPFLN, the proposed method, in which CFEU module classify the samples by Real + 1 vs. Rest perspective.

As shown in Table 2, CDCN-rs has a significant decline in performance compared with CDCN. This decline comes from the fact that CDCN is good at extracting depth information as clues to classify the positive and negative samples, but such clues could not distinguish real faces well from the newly introduced mask samples. On the contrary, setting masks as negative samples will lead to confusion of the depth estimation, resulting in the weakening of extracted features’ discrimination. This experimental result supports our assumption of model performance’s degradation because of the introduction of new attack types. Furthermore, the performance of MPFLN-rs improves over CDCN-rs due to the added 3D-CDCN structure and Model Stacking strategy. However, although the performance of MPFLN-rs is improved compared to CDCN-rs, it is still much lower than MPFLN, suggesting that the alleviation on feature discrimination’s decline is indeed due to the strategy of extracting features by group-level classification on multiple perspectives, rather than Model Stacking strategy.

5. Conclusions

In this paper, we design a Multi-Perspective Features Learning method to extract the representative features from multiple perspectives by Real+1 vs. Rest group level classifying. Based on this method, we design a neural network named Multi-Perspective Features Learning Network (MPFLN), which learned features from Real+Mask and Real+Video perspectives to perform PAD. Experiments prove the effectiveness of the proposed strategy and the model.

The possible future directions include: 1) We only performed experiments on OULU-NPU and proved the effectiveness of our method, but the studies on other datasets are still necessary; 2) Although we designed MPFLN+ to improve the performance on protocol 4, experiments on other protocols should still be performed. 3) The method of Multi-Perspective Features Learning could theoretically be extended to any backbone network or any number of attack types, which has not yet been proven.

Acknowledgements

This work was supported by the Beijing Municipal Education Committee Science Foundation under Grant K-M201910005024, and the Beijing Postdoctoral Research Foundation under Grant Q6042001202101.

References


