Adaptive Mixture of Experts Learning for Generalizable Face Anti-Spoofing

Qianyu Zhou†
Shanghai Jiao Tong University
Shanghai, China
zhouqianyu@sjtu.edu.cn

Ke-Yue Zhang∗
Youtu Lab, Tencent
Shanghai, China
zkyezhang@tencent.com

Taiping Yao∗
Youtu Lab, Tencent
Shanghai, China
taipingyao@tencent.com

Ran Yi
Shanghai Jiao Tong University
Shanghai, China
ranyi@sjtu.edu.cn

Shouhong Ding‡
Youtu Lab, Tencent
Shanghai, China
ericshding@tencent.com

Lizhuang Ma‡
Shanghai Jiao Tong University
Shanghai, China
ma-lz@cs.sjtu.edu.cn

ABSTRACT
With various face presentation attacks emerging continually, face anti-spoofing (FAS) approaches based on domain generalization (DG) have drawn growing attention. Existing DG-based FAS approaches always capture the domain-invariant features for generalizing on the various unseen domains. However, they neglect individual source domains’ discriminative characteristics and diverse domain-specific information of the unseen domains, and the trained model is not sufficient to be adapted to various unseen domains. To address this issue, we propose an Adaptive Mixture of Experts Learning (AMEL) framework, which exploits the domain-specific information to adaptively establish the link among the seen source domains and unseen target domains to further improve the generalization. Concretely, Domain-Specific Experts (DSE) are designed to investigate discriminative and unique domain-specific features as a complement to common domain-invariant features. Moreover, Dynamic Expert Aggregation (DEA) is proposed to adaptively aggregate the complementary information of each source expert based on the domain relevance to the unseen target domain. And combined with meta-learning, these modules work collaboratively to adaptively aggregate meaningful domain-specific information for the various unseen target domains. Extensive experiments and visualizations demonstrate the effectiveness of our method against the state-of-the-art competitors.

CCS CONCEPTS
• Computing methodologies → Computer vision.

1 INTRODUCTION
Face recognition (FR) techniques [11, 26, 50, 72] have been widely utilized in identity authentication products, e.g., smartphones login, access control, entrance guard systems, etc. Although FR systems
bring great convenience, they are vulnerable to various face presentation attacks (PA), e.g., printed photo, video replay, and 3D masks. As such, face anti-spoofing (FAS) has been actively studied in recent years to detect these face presentation attacks, e.g., using hand-crafted features [4, 10, 29, 40, 44, 58], deep-learning based features with binary-classification supervision [15, 21, 32, 43] or other auxiliary supervision [33, 60, 61, 65, 67]. Although these methods achieve promising performance under intra-dataset scenarios, they often suffer from performance degradation when adapting to unseen domains due to the domain gap across different domains.

To improve the generalization, recent studies [7, 24, 34, 35, 45, 46] introduce the domain generalization (DG) techniques into FAS tasks. Based on the adversarial learning or meta-learning strategies, these DG-based FAS approaches endeavor to learn the domain-invariant features in a common feature space for generalizing to unseen target domains, as shown in Figure 1 (a). However, existing DG-based FAS methods suffer from two weaknesses: 1) without considering the diverse domain-specific information of the target domains, the trained models are not sufficient to be adapted to various target domains; 2) they often neglect individual source domains’ discriminative characteristics, which provides complementary and meaningful information especially when the unseen target domain is closely related to the source domains.

To address these issues, we propose a novel perspective of generalizable face anti-spoofing that exploits the domain-specific information to adaptively establish the link between the seen source and unseen target domains to further improve the generalization, as shown in Figure 1 (b). Inspired by the works on mixture of experts (MoE) [20, 70], we propose Adaptive Mixture of Experts Learning (AMEL), a novel framework for generalizable face anti-spoofing. Specifically, we first learn the common domain-invariant features using a shared backbone with an instance normalization layer to mitigate the impact of domain information. Then, Domain-Specific Experts (DSE) are designed to investigate discriminative and unique domain-specific features as a complement to common domain-invariant features. Moreover, in order to establish the link with unseen target domains, Dynamic Expert Aggregation (DEA) is further proposed to adaptively aggregate the complementary information of each source expert based on the domain relevance w.r.t. the unseen target domain. Furthermore, to simulate diverse target domains, we introduce the meta-learning strategy and a feature consistency loss to facilitate DSE to learn complementary meaningful information for the target domain and DEA to generate suitable aggregated weights. DSE contains several small residual blocks with a few parameters to ensure high efficiency. As such, the proposed DSE and DEA work collaboratively to adaptively aggregate the specific information of the corresponding useful source domains for various unseen target domains, tackling the domain generalization issue in FAS. And to the best of our knowledge, this is the first work that treats generalizable FAS as a novel adaptive mixture of domain-specific experts paradigm.

Our contribution are summarized as follows:

- Combined with the meta-learning strategy and the feature consistency loss, Domain-Specific Experts (DSE) and Dynamic Expert Aggregation (DEA) are specifically designed to adaptively integrate source domain experts’ discriminative and meaningful information for various unseen target domains.
- Extensive experiments and visualizations are presented to reveal the role of domain-specific information utilization, which demonstrates the effectiveness of our method against state-of-the-art competitors on the widely-used benchmark datasets.

2 RELATED WORK

2.1 Face Anti-Spoofing

Face anti-spoofing (FAS) has been actively studied in recent years to detect face presentation attacks. Initially, researchers utilize handcrafted feature descriptors to extract information from images, such as LBP [3, 10, 40] and SIFT [44]. Considering that the facial motion may provide more discriminative information, some methods use the eyes blinking or the mouth speaking [49, 51] to detect the attacks. Given the limited representation abilities of the handcrafted features, the results of the above methods are not satisfactory. With the advent of deep learning, several approaches [15, 32, 43, 54, 57, 67] employ the convolutional neural network (CNN) to model the features, which gain larger improvements. However, these methods always treat FAS as a binary classification task and lack sufficient supervision, easily leading the model to a local optimum. Then, several methods [2, 6, 36, 37, 59, 66] attempt to introduce different auxiliary supervisions to improve the results, such as depth map [61], reflection map [27] and rppg signals [22, 33, 41, 62]. Based on such auxiliary supervisions, other approaches further explore specially-designed kernels [63, 64] or the disentanglement framework [38, 68] to extract more accurate features. Although these methods achieve promising performance under intra-dataset scenarios, where the testing data comes from a similar distribution of the training data, they still suffer from performance degradation when adapting to unseen domains due to the domain gap across different domains. To improve the performance under the cross-dataset setting, several methods introduce unsupervised domain adaptation [25, 30, 52, 53, 71] into the FAS area, while they rely on the unlabeled target domain during the training, which is always impractical in real-world scenarios.

2.2 Generalizable Face Anti-Spoofing

To address these issues, domain generalization [7, 24, 34, 35, 45, 46] aims to learn a generalized model on the source domains without using the target domains, which is more practical and challenging for FAS. Based on adversarial learning, MADDG [45] aligns all the samples from different domains to learn domain-invariant features. While SSDG [24] only maps the real samples of different domains to a common space without the fake ones. Based on meta-learning, RFM [46] aims to map the samples into a common classification space via a robust classifier and update with a more generalized optimization direction. D2AM [7] learns the domain-invariant features better by splitting the mixture source domains with maximum domain gaps. Besides, DRDG [35] and ANRL [34] adaptively adjust the weights of samples and features or the coefficients of normalization to boost the alignment. Although these methods gain a
Figure 2: The pipeline of our proposed Adaptive Mixture of Experts Learning (AMEL) framework, which consists of three key components. First, our framework contains a common backbone with a instance normalization layer to mitigate the impact of domain information and extract the domain-invariant features. Then, based on the common features, Domain-Specific Experts (DSE) contains several residual blocks $E_i$ to capture the individual domain’s discriminative features $F_i$. Moreover, Dynamic Expert Aggregation (DEA) dynamically leverage those complementary information of different domains into an aggregated feature based on the domain relevance w.r.t the unseen domain. The meta-learning strategy combined with the feature consistency loss is adopted to simulate diverse unseen domains and further improve the generalization.

better generalization via learning the domain-invariant features, they neglect the diverse domain-specific information of the unseen target domains and the trained model is still not sufficient to be adapted to various unseen domains. Besides, these methods overlook unique domain-specific information of the source domains, which may provide complementary discriminative and meaningful information for generalizing to the target domains. In contrast, our proposed method exploits the domain-specific information to adaptively establish the link among the seen source domains and unseen target domains to further improve the generalization.

### 2.3 Mixture of Experts

Mixture of experts (MoE) is first introduced in [23], which aims to learn a system composed of many separated networks (experts), where each expert learns to handle a subset of the whole dataset. Equipped with deep learning, deep MoEs have shown their superiorities in image recognition [1, 19, 54], image super-resolution [13], image generation [48], scene parsing [18], machine translation [47] and etc. Several methods [20, 70] utilize MoE to solve the domain adaptation (DA) via merging several domain experts to transfer toward the target domain. Some works [9, 56] also learn to aggregate the information from multiple domain-specific networks for generalizable person re-identification. Inspired by them, we propose a novel Adaptive Mixture of Experts Learning (AMEL) framework, consists of specially designed Domain-Specific Experts (DSE) and Dynamic Expert Aggregation (DEA) for generalizable FAS.

### 3 METHODOLOGY

#### 3.1 Notations and Overview

In the generalizable face anti-spoofing setting, we access to $K$ labeled source domains $D = \{D_k\}_{k=1}^K$, where $D_k = \{(x_{kn}^k, y_{kn}^k)\}_{n=1}^{N_k}$, $(x_{kn}^k, y_{kn}^k)$ is a labeled sample of domain $D_k$ and $N_k$ is the number of labeled images in the $k$-th domain. In this paper, $f$ denotes model functions and $F$ denotes the features.

Our proposed Adaptive Mixture of Experts Learning (AMEL) framework is shown in Figure 2, which contains three key components: a shared feature extraction backbone, Domain-Specific Experts (DSE) and Dynamic Expert Aggregation (DEA). Specifically, the shared feature extraction backbone with a instance normalization layer is responsible to mitigate the impact of domain information and extract domain-invariant features. Then, DSE is proposed to learn the discriminative and unique characteristics of each source domain as the complement to common domain-invariant features, and it contains several small residual blocks with a few parameters to ensure high efficiency. Moreover, to establish the link with unseen target domains, DEA adaptively aggregates the complementary information of each source expert based on the domain relevance with the unseen target domains. Furthermore, to simulate diverse target domains, the meta-learning strategy combined with a feature consistency loss is presented to facilitate the aggregation of complementary meaningful information for the target domain to further improve the generalization.
3.2 Domain-Specific Experts

Most existing works [7, 24, 34, 35, 45, 46] in DG FAS map the samples into a common feature space for capturing domain-invariant features to improve the generalization. However, without considering the diverse domain-specific information of the target domains, the trained models are not sufficient to be adapted to various target domains. Besides, the neglected domain-specific information of the source domains may be utilized to boost performances. In this work, the domain-specific features are the unique and complementary information of each source domain, such as domain-specific styles, and spoof-specific characteristics, which can further improve the generalization, especially when the unseen target domain is closely related to the source domains.

Specifically, we first utilize the instance normalization layer in the shared backbone to alleviate the impact of style information and learn the domain-invariant features. Then, different from the above works, we further put forth Domain-Specific Experts (DSE) to extract discriminative and unique domain-specific features as the complement to domain-invariant features to facilitate the generalization. Since training one individual model for each source domain to extract the domain-specific features requires large model parameters, the model size might become fairly large with the increase of source domains, limiting the practical deployment. Therefore, aiming to efficiently model the domain-specific features of each domain, here we implement DSE as K residual blocks, where each residual block contains a small convolution layer with a kernel size of $1 \times 1$, a batch normalization layer and an activation layer (ReLU). Since DSE is much smaller than the common backbone, it has both low additional computational costs and little tendency to overfit. The whole process of each domain expert extracting the domain-invariant and domain-specific features are as follows:

$$f_k(x) = f_0(x) + \Delta f^k_0(x),$$  \hspace{1cm} (1)

where $f_0$ represents the backbone that is shared by all source domains to learn the common domain-invariant features $F_c$ and each $\Delta f^k_0$ is modeled as residual block to adaptively extract the discriminative and unique domain-specific features $F_k$ of domain $D_k$. To ensure the common backbone and DSE extract the task-related features, a binary classification loss $L_{Cls}$ is defined as follows:

$$L_{Cls} = - \sum_{(x_n, y_n^{cls})} y_n^{cls} \log(Clse(f_k(x_n))),$$  \hspace{1cm} (2)

where $Clse$ is the Binary Classifier detecting the face presentation attacks from the real ones, as shown in Figure 2. Since prior works [34–36] reveal that depth can be utilized as auxiliary information to supervise both live and spoof faces on pixel level, we strictly follow them using a Depth Estimator $Dep$ and estimate the facial depth maps for live faces and zero maps for spoof faces to facilitate the learning of Feature Extractor. Thus, $L_{Dep}$ is formulated as follows:

$$L_{Dep} = \sum_{(x_n, y_n^{dep})} \left\|Dep(f_k(x_n)) - y_n^{dep}\right\|_2^2.$$  \hspace{1cm} (3)

As shown in Figure 2, the common backbone $f_0$ is updated via samples of all the source domains while each domain residual block $E_k$ in DSE is updated via the samples of corresponding domains $D_k$.

3.3 Dynamic Expert Aggregation

Since different source domains have different domain relevance to the source domains, it is necessary to adaptively aggregate the information of each source expert based on the domain relevance. As such, we introduce a Dynamic Expert Aggregation (DEA) to adaptively establish the links among source domains and unseen target domains. Compared to the attention mechanism [12, 14, 39] in Transformers that needs to interact token embeddings with each other, DEA instead queries the common features and only interacts with the feature of the domain experts, which largely simplifies the computation costs. In DEA, the inputs are the common feature $F_c$ and the concatenated features of experts $F_{concat}$, the output is the aggregated feature $F_{agg}$ of all these K expert features during inference or $K - 1$ expert features during meta-learning. Next, we elaborate on the aggregation of K expert features.

Specifically, we perform several steps for feature aggregation. Firstly, we concatenate each domain-specific feature of different domain experts to obtain the features $F_{concat}$:

$$F_{concat} = \text{concat}(\Delta f^1_c(x), \Delta f^2_c(x), \cdots, \Delta f^K_c(x)).$$  \hspace{1cm} (4)

Then, the global average pooling of the common features $F_c$ and $F_{concat}$ is utilized as the query feature and key feature, respectively, and $F_{concat}$ is used as a value feature to compute the aggregated feature. These query, key and value features are forwarded to the DEA module as inputs:

$$F_{agg} = \text{MaskedSoftmax}(F_c \otimes F_{concat}^T) \otimes F_{concat},$$  \hspace{1cm} (5)

where MaskedSoftmax is the softmax function based on a binary mask $M$ with shape $(B, KB)$, $B$ is the batch size, $\otimes$ denotes the matrix multiplication. As [9] reveals that softmax is better than sigmoid in the voting mechanism, we use softmax in our method. Concretely, the binary mask is generated by setting the relevant elements to value 1, and all others to value 0.

$$M(i, j) = \begin{cases} 1, & \text{if } j = KB + i, \text{For } k = 0, 1, \cdots, K \\ 0, & \text{otherwise} \end{cases}$$  \hspace{1cm} (6)

where $i \in \text{Range}(0, B), j \in \text{Range}(0, KB)$. We iterate each location to generate the mask. Note that DEA is lightweight and does not require additional parameters during the training. Given the above steps, Eq. 1 is re-written as follows:

$$f_k(x) = f_0(x) + \sum_{k=1}^{K} w^k \Delta f^k_0(x),$$  \hspace{1cm} (7)

where $w^k$ is the domain relevance between the k-th source domain and the unseen target domain. Note that we do not merely use domain-specific features to simulate target domains, but based on domain-invariant features, we use domain-specific features as additional complementary information that are beneficial for the discrimination in the target domain to improve the generalization.

3.4 Optimization Strategies

Due to the fact that meta-learning has shown its potential on enhancing the generalization abilities via the simulation of domain shifts among multi-source domains, we present a learning-to-learn strategy with a feature consistency loss to facilitate the whole framework to adaptively aggregate complementary meaningful domain-specific information for the various unseen target domains.
Here we elaborate the process of the optimization based on the meta-learning in detail, as shown in Algorithm 1. At the beginning of each episodic training iteration, we randomly split the source domains into the meta-train set \( D_{trn} \) (simulated “source domains”) and the meta-test set \( D_{val} \) (simulated “unseen target domains”) to simulate the real-world scenarios. Note that only domain-specific experts at residual blocks are updated via meta-learning strategy, while the other parameters in the base model including Feature Extractor, Binary Classifier and Depth Estimator follow the normal training process. Formally, we denote \( \theta_E \) as the parameters of domain expert blocks and \( \theta_B \) as the parameters of the base model, including the parameters of the shared Feature Extractor.

### Normal Train
Given batches sampled from all domains \( D \), we calculate \( L_B \) to update \( \theta_B \) for presentation attack detection:

\[
L_B(\theta_B, \theta_E) = \sum_{D} L_{Cls} + L_{Dep}
\]

\[
\theta_B \leftarrow \theta_B - \beta \nabla_{\theta_B} L_B(\theta_B, \theta_E)
\]

### Meta-Train
During the meta-train phase, each residual block of the DSE is optimized separately to exploit the domain-specific information of the corresponding source domain via a classification loss \( L_{Cls} \) and depth estimation loss \( L_{Dep} \) similarly as the normal train phase on the meta-train set \( D_{trn} \):

\[
L_{trn}(\theta_B, \theta_E) = \sum_{D_{trn}} L_{Cls} + L_{Dep}.
\]

We optimize the learning direction of domain experts via calculating gradients of \( L_{trn} \), which is formulated as:

\[
\theta_E' = \theta_E - \beta \nabla_{\theta_E} L_{trn}(\theta_B, \theta_E)
\]

where \( \theta_E' \) denotes the updated parameters of \( \theta_E \) after the one-step meta-training.

### Meta-Test
In the meta-test phase, the meta-test samples \( x \) from domain \( D_k \) will be forwarded to its own domain expert \( E_k \) to get a extracted feature \( F_k \), and meanwhile will be forwarded to other meta-test experts \( \{E_i\}_{i=1}^{K-1} \cup \{E_i\}_{i=K+1}^{K} \) to generate a aggregated feature \( F_{agg} \) with DEA module in Eq. 5. Inspired by [9], a feature consistency loss \( L_{con} \) is then imposed on these two latent features to push the aggregated feature \( F_{agg} \) as discriminative as the extracted feature \( E_k \), which forces the DEA modules to adaptively establish the link among the different source and target domains.

\[
L_{con} = \sum_{x_n \in D_{val}} \left\| F_{agg}(x_n) - F_{agg}(x_n) \right\|_2^2
\]

\[
L_{oal}(\theta_B, \theta_E') = \sum_{D_{val}} L_{Cls} + L_{Dep} + \lambda L_{con}.
\]

### Meta-Optimization
In each iteration of episodic training, we obtain \( L_{trn} \) and \( L_{oal} \) from meta-train and meta-test for optimization, which is formulated as below:

\[
\theta_E \leftarrow \theta_E - \gamma \nabla_{\theta_E} (L_{trn}(\theta_B, \theta_E) + L_{oal}(\theta_B, \theta_E'))
\]

In the above training strategy, \( \theta_E \) is updated via meta-learning and \( \theta_E \) is optimized in the normal training process, which not only improves the generalization of our method, but also facilitates the stability and efficiency of meta-learning. As such, the model obtains the abilities to aggregate the complementary information for generalizable face anti-spoofing.

---

### Algorithm 1: Training Procedure of AMDE

**Input:** Source domains \( D = \{ D_i \}_{i=1}^{K} \); Learning rate hyper-parameters \( \beta, \gamma \); Balance hyper-parameter \( \lambda \); MaxIter; MaxEpochs.

**Output:** Backbone feature extractor; Domain-specific experts \( \{E_i\}_{i=1}^{K} \); Classifier CIs; Depth Estimator Dep;

**for epoch = 1 to MaxEpochs do**

**for iter = 1 to MaxIterers do**

Sample \( K - 1 \) domains as meta-train set \( D_{trn} \) and the remaining domain as meta-test set \( D_{val} \).

**Normal Train:** Sample batch in \( D \);

\[
L_{base}(\theta_B, \theta_E') = \sum_{D} (L_{Cls} + L_{Dep})
\]

\[
\theta_B \leftarrow \theta_B - \beta \nabla_{\theta_B} L_{base}(\theta_B, \theta_E')
\]

**Meta-Train:** Sample batch in meta-train set \( D_{trn} \);

\[
L_{trn}(\theta_B, \theta_E') = \sum_{D_{trn}} (L_{Cls} + L_{Dep})
\]

\[
\theta_E' = \theta_E - \beta \nabla_{\theta_E} L_{trn}(\theta_B, \theta_E')
\]

**Meta-Test:** Sample batch in meta-test set \( D_{val} \);

\[
L_{oal}(\theta_B, \theta_E') = \sum_{D_{val}} (L_{Cls} + L_{Dep} + \lambda L_{con})
\]

**Meta-Optimization:**

\[
\theta_E \leftarrow \theta_E - \gamma \nabla_{\theta_E} (L_{trn}(\theta_B, \theta_E) + L_{oal}(\theta_B, \theta_E'))
\]

**end**

---

### 4 EXPERIMENTS

In this section, we first describe the experimental setup in Section 4.1, including the benchmark datasets and the implementation details. Then, in Section 4.2, we demonstrate the effectiveness of our framework compared to the state-of-the-art approaches on six benchmark datasets. Next, in Section 4.3, we conduct ablation studies to investigate the role of each component in the method. Finally, we provide detailed visualization and analysis in Section 4.4.

#### 4.1 Experimental Setting

**Datasets.** We use four public datasets that are widely-used in FAS research to evaluate the effectiveness of our method: OULU-NPU [5] (denoted as O), CASIA-MFSD [69] (denoted as C), Idiap Replay-Attack [8] (denoted as I), and MSU-MFSD [55] (denoted as M). These four datasets are collected with diverse capture devices, attack types, illumination conditions, background scenes, and races. Therefore, significant domain shifts exist among these datasets. In all experiments, we strictly follow the same protocols as previous DG methods [24, 34, 35, 45, 46] in FAS for experiments.

**Implementation Details.** Our method is implemented via PyTorch [42] on 24G NVIDIA 3090 GPUs and trained with Adam optimizer [28]. We use the same backbone MADDDG (M) as existing works [34, 35, 46]. We extract RGB channels of images, thus the input size is \( 256 \times 256 \times 3 \). For training, the hyper-parameter \( \lambda \) is set to 0.1 respectively. Both learning rates \( \beta \) and \( \gamma \) are set to 0.0001. Following prior works [34, 35], we utilize the PRNet [16] to generate the pseudo-depth maps. The Half Total Error Rate (HTER) and the Area Under Curve (AUC) are used as the evaluation metric [45].
Table 1: Comparison to the state-of-the-art FAS methods on four testing domains. The bold type indicates the best performance.

| Methods         | I&C&M to O | O&C&I to M | O&C&M to I | O&M&I to C |
|-----------------|------------|------------|------------|------------|
| HTER(%) AUC(%)  | HTER(%) AUC(%) | HTER(%) AUC(%) | HTER(%) AUC(%) | HTER(%) AUC(%) |
| IDA [55]        | 54.20 44.59 | 66.67 27.86 | 28.35 78.25 | 55.17 39.05 |
| LBPTOP [17]     | 53.15 44.09 | 36.90 70.80 | 49.45 49.54 | 42.60 61.05 |
| MS_LBP [40]     | 50.29 49.31 | 29.76 78.50 | 50.30 51.64 | 54.28 44.98 |
| ColorTexture [4]| 63.59 32.71 | 28.09 78.47 | 40.40 62.78 | 30.58 76.89 |
| Binary CNN      | 29.61 77.54 | 29.25 82.87 | 34.47 65.88 | 34.88 71.94 |
| Auxiliary (ALL) [36] | - - | - - | 27.60 - | 28.40 - |
| Auxiliary (Depth) [36] | 30.17 77.61 | 22.72 85.88 | 29.14 71.69 | 33.52 73.15 |
| MMD-AAE [31]    | 40.98 63.08 | 27.08 83.19 | 31.58 75.18 | 44.59 58.29 |
| MADDG [45]      | 27.98 80.02 | 17.69 88.06 | 22.19 84.99 | 24.50 84.51 |
| RFM [46]        | 16.45 91.16 | 13.89 93.98 | 17.30 90.48 | 20.27 88.16 |
| SSDG-M [24]     | 25.17 81.83 | 16.67 90.47 | 18.21 94.61 | 23.11 85.45 |
| D^2AM [7]       | 15.27 90.87 | 12.70 95.66 | 15.43 91.22 | 20.98 85.58 |
| DRDG [35]       | 15.63 91.75 | 12.43 95.81 | 15.56 91.79 | 19.05 88.79 |
| ANRL [34]       | 15.67 91.90 | 10.83 96.75 | 16.03 91.04 | 17.85 89.26 |

Ours (AMEL) | **11.31** | **93.96** | **10.23** | **96.62** | **18.60** | **88.79** | **11.88** | **94.39**

Table 2: Comparison results on limited source domains.

| Methods         | M&I to C | M&I to O |
|-----------------|----------|----------|
| HTER(%) AUC(%)  | HTER(%) AUC(%) |
| MS_LBP [40]     | 51.16 52.09 | 43.63 58.07 |
| IDA [55]        | 45.16 58.80 | 54.52 42.17 |
| Color Texture [4]| 55.17 46.89 | 53.31 45.16 |
| LBPTOP [17]     | 45.27 54.88 | 47.26 50.21 |
| MADDG [45]      | 41.02 64.33 | 39.35 65.10 |
| SSDG-M [24]     | 31.89 71.29 | 36.01 66.88 |
| D^2AM [7]       | 32.65 72.04 | 27.70 75.36 |
| DRDG [35]       | 32.18 75.10 | 33.35 69.14 |
| ANRL [34]       | 31.06 72.12 | 30.73 74.10 |

Ours (AMEL) | **23.33** | **85.17** | **19.68** | **87.01**

4.2 Comparison to the State-of-the-art Methods

To validate the generalization capability towards the unseen target domain on the FAS task, we perform two experiments following common DG FAS protocols, i.e., Leave-One-Out (LOO) generalization and generalization with limited source domains, respectively.

Comparisons in Leave-One-Out (LOO) Setting. As shown in Table 1, we conduct cross-domain generalization in four common Leave-One-Out (LOO) settings of FAS task. We randomly select three datasets from them as source domains and the left one is treated as unseen target domain, which is unavailable during the training process. The comparison methods in Table 1 are divided into two parts: conventional FAS methods and DG-based FAS methods. From the table, we make the following observations. (1). Conventional FAS methods [4, 17, 36, 40, 55, 57] show less-desired performances than DG-based FAS methods [24, 31, 34, 35, 45, 46] under these four cross-dataset benchmarks, this is due to they do not consider learning the domain-invariant representations across domains. (2). Our method outperforms most of these DG-based methods under four test settings. The main reason is that all these methods endeavor to construct a shared feature space across different domains and they largely neglect the source domains’ discriminative and complementary characteristics, while our proposed method successfully address these two issues.

Comparisons on Limited Source Domains. As illustrated in Table 2, we also evaluate our method when extremely limited source domains (i.e., only two source datasets) are available. Following
Table 3: Ablation of each component on I&C&M to O.

| ID   | Baseline | DSE+DEA | Meta | HTER(%) | AUC(%) |
|------|----------|---------|------|---------|--------|
| I    | ✓        | -       | -    | 19.72   | 87.58  |
| II   | ✓        | ✓       | -    | 14.74   | 91.90  |
| III  | ✓        | ✓       | ✓    | 11.31   | 93.96  |

Figure 4: The t-SNE feature visualization of ablation studies.

[34, 35], MSU-MFSD (M) and ReplayAttack (I) datasets are selected as the source domains for training, and the remaining two ones, i.e., CASIA-MFSD (C) and OULU-NPU (O), respectively, are used as the target domains for testing. Our proposed method outperforms the state-of-the-art approaches by a large margin despite limited source data in this more challenging case, which powerfully verifies its efficiency and generalizability on unseen target domains.

4.3 Ablation Studies

In this section, we perform ablation experiments to investigate the contribution of each component. We also investigate the effect of different aggregation strategies, expert designs, and inference strategies to demonstrate the effectiveness. All the ablation experiments are conducted on the I&C&M to O setting.

Effectiveness of each component. Table 3 shows the ablation studies of each component. The baseline means training the MADDG backbone [34, 35, 45] with IN layers, and the results are with 19.72% HTER and 87.58% AUC. By adding DSE and DEA, we boost the HTER and AUC performance by an additional 4.98%, 4.32%, achieving 14.74% HTER and 91.90% AUC, respectively. Finally, our proposed meta-learning algorithm including the feature consistency loss can effectively lower the HTER to 11.31% and increase the AUC to 93.96%, respectively. These improvements validate the effectiveness of individual components of our proposed approach. It also reveals that these components are complementary and together they significantly promote performance.

As shown in Figure 4, we visualize the feature distributions to further demonstrate the effectiveness of each part in our proposed method. From Figure 4 (a), as for the baseline model, the source features are well-discriminated while the unseen target features are not. As shown in Figure 4 (b), by adding DSE for each domain together with DEA, the above issue is alleviated to some extent. The classification boundary becomes more clear but there are still some samples misclassified near the decision boundary since the aggregation abilities are not fully generalizable due to the lack of simulating the unseen domains. As such, by further adding meta-learning with the feature consistency loss in Figure 4 (c), our approach manages to learn a better decision boundary between these two categories.

Ablations of different expert designs. Table 4 illustrates the comparisons of different expert designs. For a lightweight design, we implement our expert with a 1×1 convolutional block, BN layer, and a relu activation. When using an IN+Conv+Relu or Conv+IN+Relu, the performance is less-desirable in terms of both HTER and AUC. The main reasons are that IN layer would filter some domain-specific information, e.g., styles, and it is not beneficial for exploring the source domains’ unique and discriminative information. Compared to them, we find Conv+BN+Relu is the best combination.

Impact of aggregation strategies. Table 5 shows the impact of different aggregation strategies on the same baseline. Average Voting means to average the domain relevance of all domain experts to make final aggregation, and Expert Ensembling means to directly sum the domain relevance of all expert branches. Max Selection means to select the maximum value of the domain relevance, in other words, the most similar source domain expert with the unseen target domain will be utilized for feeding forward. From the table, we observe that our proposed DEA outperforms these two related aggregation strategies. This is because their aggregation strategies largely overlook the domain relevance w.r.t. the unseen target domain, and naively averaging or ensembling all the source domains’ individual information is impractical.

4.4 Visualization and Analysis

Analysis of different inference strategies using the corresponding expert branch. As shown in Table 6, when using the source domain expert branch with the common feature for inference, the performance are less-desired, which indicates that only using one single source expert is not sufficient for generalization due to the large domain shifts. Besides, we can find that the not all source domains contribute equally towards the unseen target domain. For example, in I&C&M to O setting, the expert branch of C dataset could achieve better performance than others on the unseen target domain due to the domain relevance between C dataset and O dataset are higher than others. Compared to these aforementioned inference strategies, our proposed approach can achieve the best performance on four challenging benchmark datasets.
Table 6: Comparison of inference strategies on four testing domains. The bold type indicates the best performance.

| Methods                               | I&C&M to O | O&C&M to I | O&M&I to C |
|---------------------------------------|------------|------------|------------|
|                                       | HTER(%)    | AUC(%)     | HTER(%)    | AUC(%)     | HTER(%)    | AUC(%)     |
| Common feature + Expert O             | –          | –          | 17.38      | 90.89      | 28.50      | 79.04      | 16.00      | 92.45      |
| Common feature + Expert M             | 23.86      | 83.58      | –          | –          | 18.40      | 87.14      | 19.89      | 88.64      |
| Common feature + Expert I             | 29.00      | 75.75      | 22.14      | 87.27      | –          | –          | 23.56      | 86.71      |
| Common feature + Expert C             | 13.53      | 92.23      | 15.00      | 93.18      | 26.10      | 76.36      | –          | –          |
| Ours (Common feature + Aggregated feature) | **11.31** | **93.96** | **10.23** | **96.62** | **18.60** | **88.79** | **11.88** | **94.39** |

![Visualizations of expert feature and aggregated features. As shown in Figure 5, we visualize the features of each source domain expert and the aggregated feature in the I&C&M to O setting. And we can make the following observations: (1) Each domain expert learns differently, and those source samples that share more similarities with the unseen target samples will provide more meaningful and discriminative information for enhance the generalization. For example, in the third row, the expert of domain I and domain C pay attention to the eye region, while the expert of domain M ignores the region. (2) Since each sample in the domain O has different similarities with three different source domains, the weights of each samples are various, which further confirms that our method could dynamically utilize the specific source information to adaptively simulate the domain-specific features of the unseen target domain. The t-SNE visualization of features.](image).

Figure 6: The t-SNE visualization of common features and aggregated features on I&C&M to O setting.

Visualizations of expert feature and aggregated features. As shown in Figure 5, we visualize the features of each source domain expert and the aggregated feature in the I&C&M to O setting. And we can make the following observations: (1) Each domain expert learns differently, and those source samples that share more similarities with the unseen target samples will provide more meaningful and discriminative information for enhance the generalization. For example, in the third row, the expert of domain I and domain C pay attention to the eye region, while the expert of domain M ignores the region. (2) Since each sample in the domain O has different similarities with three different source domains, the weights of each samples are various, which further confirms that our method could dynamically utilize the specific source information to adaptively simulate the domain-specific features of the unseen target domain.

The t-SNE visualization of features. To understand how the AMEL framework aligns the feature, we utilize t-SNE to visualize the feature distributions of each domain, including three source domains and the unseen target domain in the I&C&M to O setting. We can make the following two observations: (1) When using the common feature for generalization, as shown in Figure 6(a), the source data can be well discriminated by binary classification. However, the target data is not well-classified near the decision boundary. Instead, in Figure 6(b) our approach manages to learn a better decision boundary between these two categories of real and attack samples. (2) Besides, the common features of the same category are more compact, while the distributions of aggregated feature are looser. The main reason is that merely learning the domain-invariant feature in the common feature space is not sufficient for domain generalization, and those discriminative and unique domain-specific features could improve the performance as a useful complement to the common domain-invariant features.

5 CONCLUSION

In this paper, we present a novel Adaptive Mixture of Experts Learning (AMEL) framework to address the generalizable face anti-Spoofing, which exploits the domain-specific information to adaptively establish the link between the seen source and unseen target domains to further improve the generalization. Specifically, Domain-Specific Experts (DSE) are trained to learn the individual domain’s discriminative feature. Besides, Dynamic Expert Aggregation (DEA) is presented to dynamically leverage complementary information of different domains into an aggregated feature based on the domain relevance w.r.t. the unseen domain. Finally, to enhance the model generalizability, we present a meta-learning algorithm with a feature consistency loss to simulate the domain-specific feature of the unseen target domain. Extensive experiments with analysis demonstrate the effectiveness of our proposed approach.

ACKNOWLEDGMENTS

This work is supported by National Key Research and Development Program of China (2019YFC1521104), National Natural Science Foundation of China (72192821, 61972157), Shanghai Municipal Science and Technology Major Project (2021SHZDZX0102), Shanghai Science and Technology Commission (21511101200, 22YF1420300), and Art major project of National Social Science Fund (I8ZD22).
REFERENCES

[1] Karim Ahmed, Mohammad Haris Baig, and Lorenzo Torresani. 2016. Network of experts for large-scale image categorization. In European Conference on Computer Vision. Springer, 532.

[2] Youssef Atoum, Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. 2018. Face Anti-Spoofing using Patch and Depth-based CNNs. In Proceedings of the IEEE International Conference on Biometrics (IJCB).

[3] Zinelalbide Boulenafet, Jukka Komulainen, and Abdounour Hadid. 2015. Face anti-spoofing based on color texture analysis. In International Conference on Image Processing (ICIP).

[4] Zinelalbide Boulenafet, Jukka Komulainen, and Abdounour Hadid. 2017. Face Spoofing Detection using Colour Texture Analysis. IEEE Transactions on Information Forensics and Security (TIFS) 13.1 (2018), 1816–1830.

[5] Zinelalbide Boulenafet, Jukka Komulainen, Lei Li, Xiaoai Feng, and Abdounor Hadid. 2017. OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations. In Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition (FG).

[6] Shen Chen, Taiping Yao, Ke-Yue Zhang, Yang Chen, Ke Sun, Shouhong Ding, Jilin Li, Feiyue Huang, and Rongrong Ji. 2021. A dual-stream framework for 3D Mask Face Presentation Attack Detection. In Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV). 834–841.

[7] Zhuhong Chen, Taiping Yao, Kekai Sheng, Shouhong Ding, Ying Tai, Jilin Li, Feiyue Huang, and Xinyu Jin. 2021. Generalizable Representation Learning for Mixed Domain Face Anti-Spoofing. Proceedings of the AAAI Conference on Artificial Intelligence (AAAI) (2021).

[8] Ivana Chingovska, André Anjos, and Sébastien Marcel. 2012. On the effectiveness of local binary patterns in face anti-spoofing. In International Conference of Biometrics Special Interest Group. IEEE, 1–7.

[9] Yongxing Dai, Xiaotong Li, Jun Liu, Zekun Tong, and Ling-Yu Duan. 2021. Generalizable person re-identification with relevance-aware mixture of experts. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 16145–16154.

[10] Tiago de Freitas Pereira, André Anjos, José Mario De Martinho, and Sébastien Marcel. 2012. LBP-TOP based countermeasure against face spoofing attacks. In Asian Conference on Computer Vision (ACCV).

[11] Jiankang Deng, Jilin Li, Nianman Xue, and Stefanos Zafeiriou. 2019. Arcface: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (CVPR). 4609–4619.

[12] Alexey Dosovitskiy, Lucas Beyer, Alexander Kolesnikov, Dirk Weissenborn, Xiaohua Zhai, Thomas Unterthiner, Mostafa Dehghani, Matthias Minderer, Georg Heigold, Sylvain Gelly, et al. 2020. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. In International Conference on Learning Representations (ICLR).

[13] Mohammad Emad, Maurice Peemen, and Henk Corporaal. 2022. MoESR: Blind learning model for face spoofing detection. arXiv preprint arXiv:1809.02256 (2019).

[14] Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. 2018. Learning Deep Models for Face Anti-Spoofing. In Proceedings of the IEEE Conference on Biometrics (ICB).

[15] Haoliang Li, Wen Li, Hong Cao, Shiqi Wang, Feiyue Huang, and Alex C. Kot. 2018. Unsupervised Domain Adaptation for Face Anti-Spoofing. IEEE Transactions on Information Forensics and Security (TIFS) 13.3 (2018), 1794–1809.

[16] Yaojie Liu, Sinno Jialin Pan, Shiqi Wang, and Alex C. Kot. 2018. Domain Generalization with Adversarial Feature Learning. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

[17] Lei Li, Xiaoai Feng, Zinelabidine Boulkenafet, Zhaoming Xia, Mingming Li, and Abdounor Hadid. 2016. An original face anti-spoofing approach using partial convolutional neural network. In International Conference on Image Processing (ICIP). 4873–4882.

[18] Yunpei Jia, Jie Zhang, Shiguang Shan, and Xilin Chen. 2020. Single-Side Domain Generalization for Face Anti-Spoofing. Proceedings of the 29th ACM International Conference on Multimedia (ACM MM) (2021).

[19] Shuang Liu, Ke-Yue Zhang, Taiping Yao, Kekai Sheng, Shouhong Ding, Ying Tai, Jilin Li, Yuan Xie, and Lizhuang Ma. 2021. Dual reweighting domain generalization for face presentation attack detection. International Joint Conference on Artificial Intelligence (IJCAI) (2021).

[20] Yaojie Liu, Amin Jourabloo, and Xiaoming Liu. 2018. Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

[21] Yaojie Liu, Joel Stehouwer, Amin Jourabloo, and Xiaoming Liu. 2019. Deep tree learning for zero-shot face anti-spoofing. In Conference on Computer Vision and Pattern Recognition (CVPR).

[22] Yaojie Liu, Joel Stehouwer, and Xiaoming Liu. 2020. On disentangling spoof trace for generic face anti-spoofing. In European Conference on Computer Vision (ECCV). Springer, 406–422.

[23] Ze Liu, Yutong Lin, Yue Cao, Han Hu, Yeuxan Wei, Zheng Zhang, Stephen Lin, and Junzhou Huang. 2021. Swin transformer: Hierarchical vision transformer using shifted windows. In Proceedings of the IEEE/CVF International Conference on Computer Vision (CVPR). 10012–10022.

[24] Jukka Maatta, Abdounor Hadid, and Matti Pietikainen. 2011. Face Spoofing Detection from Single Images using Micro-texture Analysis. In Proceedings of the IEEE International Joint Conference on Biometrics (IJCB).

[25] Xuesong Niu, Zitong Yu, Hu Han, Xiaoai Li, Shiguang Shan, and Guoying Zhao. 2020. Video-based Remote Physiological Measurement via Cross-verified Feature Disentangling. In European Conference on Computer Vision (ECCV).

[26] Adas Adamczewski, Paul Infeld, and Tero Sasing. 2019. Meta learning for face anti-spoofing. In Proceedings of the IEEE Conference on Biometric Recognition (CBIR).

[27] Adas Adamczewski, Paul Infeld, and Tero Sasing. 2019. Secure Face Unlock: Spoofer Detection on Smartphones. IEEE Transactions on Information Forensics and Security (TIFS) 11, 10 (2016), 2268–2283.

[28] Ruixiang Shao, Xiangyuan Lan, Jifeng Li, and Pong C. Yuen. 2019. Meta-Adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

[29] Rui Shao, Xiangyuan Lan, and Pong C. Yuen. 2020. Regularized Fine-Gained Meta Face Anti-Spoofing. In Proceedings of the AAAI Conference on Artificial Intelligence (AAAI).

[30] Noam Shazeer, Azalia Mirhoseini, Krzysztof Maziarz, Andy Davis, Quoc Le, Geoffrey Hinton, and Jeff Dean. 2017. Outrageously large neural networks: The revisited M6.
Yuge Shi, Brooks Paige, Philip Torr, et al. 2019. Variational mixture-of-experts autoencoders for multi-modal deep generative models. Advances in Neural Information Processing Systems (NeurIPS) 32 (2019).

Talha Ahmad Siddiqui, Samarth Bharadwaj, Tejas I Dhamneca, Akshay Agarwal, Mayank Vatsa, Richa Singh, and Nalini Ratha. 2016. Face anti-spoofing with multifeature videodetected aggregation. In 2016 23rd International Conference on Pattern Recognition (ICPR). IEEE, 1035–1040.

Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. 2014. Deepface: Closing the gap to human-level performance in face verification. In Proceedings of the IEEE conference on computer vision and pattern recognition (CVPR). 1701–1708.

Di Wen, Hu Han, and Anil K. Jain. 2015. Face Spoof Detection with Image Data. In Proceedings of the IEEE International Conference on Biometrics (ICB).

Guoqing Wang, Hu Han, Shiguang Shan, and Xilin Chen. 2021. Unsupervised Adversarial Domain Adaptation for Cross-Domain Face Presentation Attack Detection. IEEE Transactions on Information Forensics and Security (TIFS) 16 (2021), 56–69.

Zhengsheng Wang, Zitong Yu, Chenxu Zhao, Xiangyu Zhu, Yunxiao Qin, Qingsheng Zhou, Peng Zhou, and Zhen Lei. 2020. Deep spatial gradient and temporal depth learning for face anti-spoofing. In Conference on Computer Vision and Pattern Recognition (CVPR).

Di Wen, Hu Han, and Anil K. Jain. 2015. Face Spoof Detection with Image Distortion Analysis. IEEE Transactions on Information Forensics and Security (TIFS) 10, 4 (2015), 746–761.

Yichao Yan, Junjie Li, Shengcai Liao, Jie Qin, Bingbing Hong, and Xiaokang Yang. 2021. TAL: Two-stream Adaptive Learning for Generalizable Person Recognition. IEEE Transactions on Information Forensics and Security (TIFS) 16 (2021), 56–69.

Jianwei Yang, Zhen Lei, and Stan Z Li. 2014. Learn Convolutional Neural Network architecture. In Proceedings of the IEEE International Conference on Biometrics (ICB).

Xiaoguang Tu, Hengsheng Zhang, Mei Xie, Yao Luo, Yuefei Zhang, and Zheng Ma. 2019. Enhance the motion cues for face anti-spoofing using CNN-LSTM architecture. arXiv preprint arXiv:1901.05635 (2019).

Guoqing Wang, Hu Han, Shiguang Shan, and Xilin Chen. 2019. Improving Cross-Domain Face Presentation Attack Detection via Adversarial Domain Adaptation. In Proceedings of the IEEE International Conference on Biometrics (ICB).

Zitong Yu, Yunxiao Qin, Xiaobai Li, Xiaopeng Hong, and Guoying Zhao. 2019. Remote heart rate measurement from highly compressed facial videos: an end-to-end deep learning solution with video enhancement. In International Conference on Computer Vision (ICCV).

Zitong Yu, Yunxiao Qin, Xiaobai Li, Ziqheng Wang, Chenxu Zhao, Zhen Lei, and Guoying Zhao. 2020. Multi-Modal Face Anti-Spoofing Based on Central Difference Networks. In Conference on Computer Vision and Pattern Recognition Workshops (CVPRW).

Zitong Yu, Yunxiao Qin, Hengshuang Zhao, Xiaobai Li, and Guoying Zhao. 2021. Dual-Cross Central Difference Network for Face Anti-Spoofing. In International Joint Conference on Artificial Intelligence (IJCAI).

Zitong Yu, Chenxu Zhao, Zicheng Wang, Yunxia Qin, Zhuo Su, Xiaobai Li, Feng Zhou, and Guoying Zhao. 2020. Searching central difference convolutional networks for face anti-spoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 5295–5305.

Jian Zhang, Ying Tai, Taiping Yao, Jia Meng, Shouhong Ding, Chengjie Wang, Jilin Li, Feiyue Huang, and Rongrong Ji. 2021. Aurora Guard: Reliable Face Anti-Spoofing via Mobile Lighting System. arXiv preprint arXiv:2102.00713.

Ke-Yue Zhang, Taiping Yao, Jian Zhang, Shicke Liu, Bangjie Yin, Shouhong Ding, and Jilin Li. 2021. Structure destruction and content combination for face anti-spoofing. In 2021 IEEE International Joint Conference on Biometrics (IJCB). IEEE, 1–6.

Ke-Yue Zhang, Taiping Yao, Jian Zhang, Ying Tai, Shouhong Ding, Jilin Li, Feiyue Huang, Haichuan Song, and Lizhuang Ma. 2020. Face anti-spoofing via disentangled representation learning. In European Conference on Computer Vision (ECCV). Springer, 641–657.

Zhiwei Zhang, Junjie Yan, Sifei Liu, Lei Zhen, and Stan Z Li. 2012. A Face Anti-Spoofing Database with Diverse Attacks. In Proceedings of the IEEE International Conference on Biometrics (ICB).

Kaiyang Zhou, Ke-Yue Zhang, Taiping Yao, Ran Yi, Kekai Sheng, Shouhong Ding, and Lizhuang Ma. 2022. Generative domain adaptation for face anti-spoofing. In European Conference on Computer Vision (ECCV). Springer.

Qianyu Zhou, Ke-Yue Zhang, Taiping Yao, Ran Yi, Kekai Sheng, Shouhong Ding, and Lizhuang Ma. 2022. Generative domain adaptation for face anti-spoofing. In European Conference on Computer Vision (ECCV). Springer.

Wenbin Zhu, Chien-Yi Wang, Kuan-Lun Tseng, Shang-Hong Lai, and Baoyuan Wang. 2022. Local-Adaptive Face Recognition via Graph-based Meta-Clustering and Regularized Adaptation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 20301–20310.