Regularized Fine-grained Meta Face Anti-spoofing

Rui Shao, Xiangyuan Lan, Pong C. Yuen

Department of Computer Science, Hong Kong Baptist University, Hong Kong

{ruishao, pcyuen}@comp.hkbu.edu.hk, xiangyuanlan@life.hkbu.edu.hk

Abstract

Face presentation attacks have become an increasingly critical concern when face recognition is widely applied. Many face anti-spoofing methods have been proposed, but most of them ignore the generalization ability to unseen attacks. To overcome the limitation, this work casts face anti-spoofing as a domain generalization (DG) problem, and attempts to address this problem by developing a new meta-learning framework called Regularized Fine-grained Meta-learning. To let our face anti-spoofing model generalize well to unseen attacks, the proposed framework trains our model to perform well in the simulated domain shift scenarios, which is achieved by finding generalized learning directions in the meta-learning process. Specifically, the proposed framework incorporates the domain knowledge of face anti-spoofing as the regularization so that meta-learning is conducted in the feature space regularized by the supervision of domain knowledge. This enables our model more likely to find generalized learning directions with the regularized meta-learning for face anti-spoofing task. Besides, to further enhance the generalization ability of our model, the proposed framework adopts a fine-grained learning strategy that simultaneously conducts meta-learning in a variety of domain shift scenarios in each iteration. Extensive experiments on four public datasets validate the effectiveness of the proposed method.

Introduction

Face recognition, as one of the computer vision techniques (Lan et al. 2019; Ye et al. 2019), has been successfully applied in a variety of applications in the real life, such as automated teller machines (ATMs), mobile payments, and entrance guard systems. Although much convenience is brought by the face recognition technique, many kinds of face presentation attacks (PA) also appear. Easy-accessible human faces from the Internet or social media can be abused to produce print attacks (i.e. based on the printed photo papers) or video replay attacks (i.e. based on the digital image/videos). These attacks can successfully hack a face recognition system deployed in a mobile phone or a laptop because those spoofs are visually extremely close to the genuine faces. Therefore, how to protect our face recognition
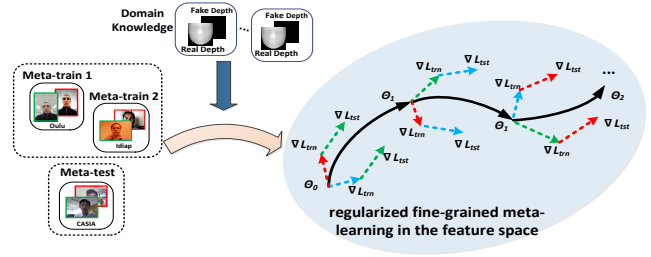
Figure 1: Idea of the proposed regularized fine-grained meta-learning framework. By incorporating domain knowledge as regularization, meta-learning is conducted in the feature space regularized by the domain knowledge supervision. Thus, generalized learning directions are more likely to be found for task of face anti-spoofing. Besides, the proposed framework adopts a fine-grained learning strategy that simultaneously conducts meta-learning in a variety of domain shift scenarios. Thus, more abundant domain shift information of face anti-spoofing task can be exploited.

systems against these presentation attacks has become an increasingly critical issue in the face recognition community.

Many face anti-spoofing methods have been proposed. Appearance-based methods choose to extract various appearance cues to differentiate real and fake (Boulkenafet, Komulainen, and Hadid 2016; 2016; Wen, Han, and Jain 2015; Yang, Lei, and Li 2014); Temporal-based methods aim to do differentiation based on various temporal cues (Pereira and et al 2014; Shao, Lan, and Yuen 2019; 2017; Liu, Lan, and Yuen 2018; Liu, Jourabloo, and Liu 2018). Although these methods obtain promising performance in intra-dataset experiments where training and testing data are from the same dataset, the performance dramatically degrades in cross-dataset experiments where models are trained on one dataset and tested on a related but shifted dataset. This is because existing face anti-spoofing methods capture the differentiation cues that are dataset biased (Antonio and Efros 2011), and thus cannot generalize well to unseen testing data that have different feature distribution compared to training data (mainly caused by different mate-

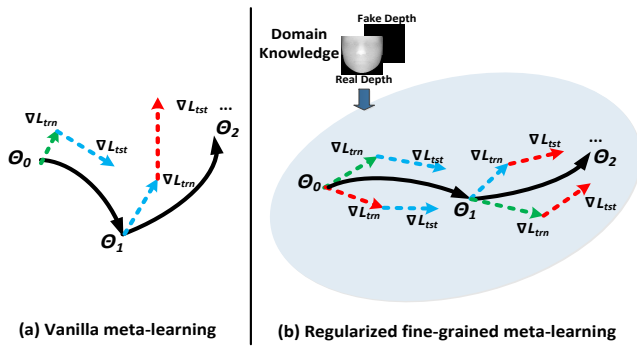**(a) Vanilla meta-learning** | **(b) Regularized fine-grained meta-learning**

Figure 2: Comparison of learning directions between (a) vanilla meta-learning, and (b) regularized fine-grained meta-learning. Three source domains are used as examples. Dotted arrows with different colors denote the learning directions (gradients) of meta-train (∇L_{trn}) and meta-test (∇L_{tst}) in different domains. Solid arrows denote the summarized learning directions of meta-optimization. θ_i ($i = 0, 1, ...$) are the updated model parameters in i-th iteration.

rials of attacks or recording environments).

To overcome this limitation, this paper casts face anti-spoofing as a domain generalization (DG) problem. Compared to the traditional unsupervised domain adaptation (UDA) (Shao, Lan, and Yuen 2018; Saito et al. 2018; Mancini et al. 2018; Zhang et al. 2018b; Chen et al. 2018; Pinheiro 2018; Tzeng et al. 2017; Bousmalis et al. 2017; Volpi et al. 2018; Zhang et al. 2018a; Bhushan Damodaran, Kellenberger, and et al 2018; Shao and Lan 2019) that assume access to the labeled source domain data and unlabeled target domain data, DG assumes no access to target domain information. For DG, multiple source domains are exploited to learn the model which can generalize well to unseen test data in the target domain. For the task of face anti-spoofing, because we do not know what kind of attacks will be presented to our face recognition system, we have no clue on the testing dataset (target domain data) when we train our model so that DG is more suitable for our task.

Inspired by (Finn, Abbeel, and Levine 2017; Li et al. 2018a), this paper aims to address problem of DG for face anti-spoofing in a *meta-learning* framework. However, if we directly apply existing vanilla meta-learning for DG algorithms on the task of face anti-spoofing, the performance will be degraded due to the following two issues: 1) It is found that face anti-spoofing models only with binary class supervision discover arbitrary differentiation cues with poor generalization (Liu, Jourabloo, and Liu 2018). As such, as illustrated in Fig. 2(a), if vanilla meta-learning algorithms are applied in face anti-spoofing only with the supervision of the binary class labels, the learning directions in the meta-train and meta-test steps will be arbitrary and biased, which makes it difficult for the meta-optimization step to summarize and find a generalized learning direction finally. 2) Vanilla meta-learning for DG methods (Li et al. 2018a) coarsely divide multiple source domains into two groups to form one aggregated meta-train and one aggregated meta-test domains in each iteration of meta-learning. Thus only a single domain shift scenario is simulated in each iteration, which is sub-optimal for the task of face anti-spoofing. In order to equip the model with the generalization ability to unseen attacks of various scenarios, a variety of domain shift scenarios instead of a single one that are simulated for meta-learning is more optimal for the task of face anti-spoofing.

To address the above two issues, as illustrated in Fig. 1, this paper proposes a novel regularized fine-grained meta-learning framework. For the first issue, compared to binary class labels, domain knowledge specific to the task of face anti-spoofing can provide more generalized differentiation information. Therefore, as illustrated in Fig .2(b), the proposed framework incorporates the domain knowledge of face anti-spoofing as regularization into feature learning process so that meta-learning is conducted in the feature space regularized by the auxiliary supervision of domain knowledge. In this way, this regularized meta-learning can focus on more coordinated and better-generalized learning directions in the meta-train and meta-test for task of face anti-spoofing. Therefore, the summarized learning direction in the meta-optimization can guide face anti-spoofing model to exploit more generalized differentiation cues. Besides, for the second issue, the proposed framework adopts a fine-grained learning strategy as shown in Fig .2(b). This strategy divides source domains into multiple meta-train and meta-test domains, and jointly conducts meta-learning between each pair of them in each iteration. As such, a variety of domain shift scenarios are simultaneously simulated and thus more abundant domain shift information can be exploited in the meta-learning to train a generalized face anti-spoofing model.

Related Work

Face Anti-spoofing Methods. Current face anti-spoofing methods can be roughly categorized into appearance-based methods and temporal-based methods. Appearance-based methods are proposed to extract different appearance cues for attacks detection. Multi-scale LBP (Määttä, Hadid, and Pietikäinen 2011) and color textures (Boulkenafet, Komulainen, and Hadid 2016) methods are proposed to extract various LBP descriptors in various color spaces for the differentiation between real/fake. Image distortion analysis (Wen, Han, and Jain 2015) detects the surface distortions due to lower appearance quality of images or videos compared to the real face skin. Yang *et al.* (Yang, Lei, and Li. 2014) trains CNN to extract discriminative deep features for real/fake faces classification. On the other hand, temporal-based methods aim to extract different temporal cues through multiple frames to differentiate real/fake faces. Dynamic texture methods proposed in (Pereira and et al 2014; Shao, Lan, and Yuen 2019; 2017) try to extract different facial motions. Liu *et al.* (Liu et al. 2016; Liu, Lan, and Yuen 2018) propose to capture discriminative rPPG signals from real/fake faces. (Liu, Jourabloo, and Liu 2018) learns a CNN-RNN model to estimate the different face depth and rPPG signals between real/fake faces. However, the performance of both appearance and temporal-based methods become degraded in cross-datasets test where
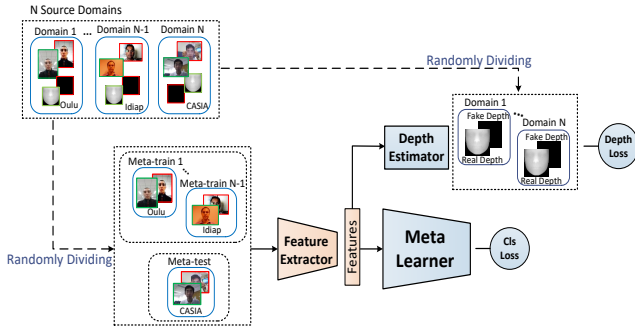
Figure 3: Overview of proposed framework. We simulate domain shift by randomly dividing original N source domains in each iteration. Supervision of domain knowledge is incorporated via depth estimator to regularize the learning process of feature extractor. Thus, meta learner conducts the meta-learning in the feature space regularized by the auxiliary supervision of domain knowledge.

unseen attacks are encountered. This is because all the above methods are likely to extract some differentiation cues that are biased to specific materials of attacks or recording environments in training datasets. Comparatively, the proposed method conducts meta-learning for DG in the simulated domain shift scenarios, which is designed to make our model generalize well and capture more generalized differentiation cues for the task of face anti-spoofing. Note that a recent work (Shao et al. 2019) proposes multi-adversarial discriminative deep domain generalization for face anti-spoofing. It assumes that generalized differentiation cues can be discovered by searching a shared and discriminative feature space via adversarial learning. However, there is no guarantee that such a feature space exists among multiple source domains. Moreover, it needs to train multiple extra discriminators for all source domains. Comparatively, this paper does not need such a strong assumption and meta-learning can be conducted without training extra discriminators networks for adversarial learning, which is more efficient.

Meta-learning for Domain Generalization Methods.
Unlike meta-learning for few-shot learning (Finn, Abbeel, and Levine 2017), meta-learning for DG is relatively less explored. MLDG (Li et al. 2018a) designs a model-agnostic meta-learning for DG. Reptile (Nichol, Achiam, and Schulman. 2018) is a general first-order meta-learning method that can be easily adapted into DG task. MetaReg (Balaji and et al 2018) learns regularizers for DG in a meta-learning framework. However, directly applying the aforementioned methods in the task of face anti-spoofing may encounter the two issues mentioned above. Comparatively, our method conducts meta-learning in the feature space regularized by auxiliary supervision of domain knowledge within a fine-grained learning strategy. This contributes a more feasible meta-learning for DG in the task of face anti-spoofing.

Proposed Method

The overall proposed framework is illustrated in Fig. 3.

Domain Shift Simulating

Suppose that we have access to N source domains of face anti-spoofing task, denoted as $D = [D_1, D_2, ..., D_N]$. The objective of DG for face anti-spoofing is to make the model trained on the N source domains can generalize well to unseen attacks from the target domain. To this end, at each training iteration, we divide the original N source domains by randomly selecting $N-1$ domains as meta-train domains (denoted as D_{trn}) and the remaining one as the meta-test domain (denoted as D_{val}). As such, the training and testing domain shift in the real world can be simulated. In this way, our model can learn how to perform well in the domain shift scenarios through many training iterations and thus learn to generalize well to unseen attacks.

Regularized Fine-grained Meta-learning

Several existing vanilla meta-learning for DG methods can be applied to achieve the above objective. But their performance degrade for the task of face anti-spoofing due to the two issues mentioned in the introduction. To address these issues, this paper proposes a new meta-learning framework called regularized fine-grained meta-learning. In each meta-train and meta-test domain, we are provided with image and label pairs denoted as x and y, where y are ground truth with binary class labels ($y = 0/1$ is the label of fake/real face). Compared to the binary class labels, domain knowledge specific to the face anti-spoofing task can provide more generalized differentiation information. This paper adopts the face depth map as the domain knowledge. By comparing the spatial information, it can be observed that live faces have face-like depth, while faces of attacks presented in the flat and planar papers or video screens have no face depth. In this way, for the first issue, we incorporate this domain knowledge as regularization into feature learning process so that meta-learning can be conducted in the feature space regularized by the auxiliary supervision of domain knowledge. Thus, this regularized meta-learning in the feature space can focus on better-generalized learning directions in meta-train and meta-test for task of face anti-spoofing. To this end, as illustrated in Fig. 3, a convolutional neural network is proposed in our framework that composes of a feature extractor (denoted as F) and a meta learner (denoted as M). Then a depth estimator (denoted as D) is further integrated into our network, through which domain knowledge can be incorporated. Besides, to address the second issue, the proposed framework adopts a fine-grained learning strategy that meta-learning is jointly conducted among $N-1$ meta-train domains and one meta-test domain in each iteration, by which a variety of domain shift scenarios are simultaneously exploited in each iteration. The whole meta-learning process is summarized in Algorithm 1 and the details are as follows:

Meta-Train. We sample batches in every meta-train domain D_{trn}, denoted as $\widehat{\mathcal{T}}_i$ ($i = 1, ..., N-1$), and we conduct the cross-entropy classification based on the binary class labels in each meta-train domain as follows:

$$\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M)$$
$$= \sum_{(x,y)\sim\widehat{\mathcal{T}}_i} y\log M(F(x)) + (1-y)\log(1 - M(F(x))) \quad (1)$$

where θ_F and θ_M are the parameters of the feature extractor and the meta learner. In each meta-train domain, We can thus search the learning direction by calculating gradient of meta learner w.r.t the loss ($\nabla_{\theta_M}\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M)$). The updated meta learner can be calculated as $\theta_{M_i}' = \theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M)$. In the meantime, we incorporate face depth maps as the domain knowledge to regularize the above learning process of the feature extractor as follows:

$$\mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D) = \sum_{(x,I)\sim\widehat{\mathcal{T}}_i} \|D(F(x)) - I\|^2 \quad (2)$$

where θ_D is the parameter of the depth estimator and I are the pre-calculated face depth maps for input face images. We use the state-of-the-art dense face alignment network named PRNet (Feng et al. 2018) to estimate depth maps of real faces, which serve as the supervision for the real faces. Attacks are assumed to have no face depth so that depth maps of all zeros are set as the supervision for fake faces.

Meta-Test. Moreover, we sample batch in the one remaining meta-test domain D_{val}, denoted as $\widetilde{\mathcal{T}}$. By adopting fine-grained learning strategy, we encourage our face anti-spoofing model trained on every meta-train domain can simultaneously perform well on the disjoint meta-test domain so that our model can be trained to generalize well to unseen attacks of various scenarios. Thus, multiple cross-entropy classifications are jointly conducted over all the updated meta learners:

$$\sum_{i=1}^{N-1} \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}') =$$
$$\sum_{i=1}^{N-1} \sum_{(x,y)\sim\widetilde{\mathcal{T}}} y\log M_i'(F(x)) + (1-y)\log(1 - M_i'(F(x))) \quad (3)$$

The domain knowledge is also incorporated like meta-train:

$$\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) = \sum_{(x,I)\sim\widetilde{\mathcal{T}}} \|D(F(x)) - I\|^2 \quad (4)$$

Meta-Optimization. To summarize all the learning information in the meta-train and meta-test for optimization, we jointly train the three modules in our network as follows:

$$\theta_M \leftarrow \theta_M - \beta\nabla_{\theta_M}\left(\sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}'))\right) \quad (5)$$

$$\theta_F \leftarrow \theta_F - \beta\nabla_{\theta_F}(\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M)$$
$$+ \mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}'))) \quad (6)$$

Algorithm 1 Regularized Fine-grained Meta Face Anti-spoofing

Require:
    Input: N source domains $D = [D_1, D_2, ..., D_N]$,
    Initialization: Model parameters $\theta_F, \theta_D, \theta_M$. Hyperparameters α, β

1: **while** not done **do**
2:      Randomly select $(N-1)$ source domains in D as D_{trn}, and the remaining one as D_{val}
3:      **Meta-train:** Sampling batch in each domain in D_{trn} as $\widehat{\mathcal{T}}_i$ $(i = 1, ..., N-1)$
4:      **for** each $\widehat{\mathcal{T}}_i$ **do**
5:        $\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) = \sum_{(x,y)\sim\widehat{\mathcal{T}}_i} y\log M(F(x)) + (1-y)\log(1 - M(F(x)))$
6:        $\theta_{M_i}' = \theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M)$
7:        $\mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D) = \sum_{(x,I)\sim\widehat{\mathcal{T}}_i} \|D(F(x)) - I\|^2$
8:      **end for**
9:      **Meta-test:** Sampling batch in D_{val} as $\widetilde{\mathcal{T}}$
10:     $\sum_{i=1}^{N-1}\mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}') = \sum_{i=1}^{N-1}\sum_{(x,y)\sim\widetilde{\mathcal{T}}} y\log M_i'(F(x)) + (1-y)\log(1 - M_i'(F(x)))$
11:     $\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) = \sum_{(x,I)\sim\widetilde{\mathcal{T}}} \|D(F(x)) - I\|^2$
12:     **Meta-optimization:**
13:     $\theta_M \leftarrow \theta_M - \beta\nabla_{\theta_M}(\sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}')))$
14:     $\theta_F \leftarrow \theta_F - \beta\nabla_{\theta_F}(\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_M) + \mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_F, \theta_{M_i}')))$
15:     $\theta_D \leftarrow \theta_D - \beta\nabla_{\theta_D}(\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}(\mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D)))$
16: **end while**
17: **return** Model parameters $\theta_F, \theta_D, \theta_M$

$$\theta_D \leftarrow \theta_D - \beta\nabla_{\theta_D}(\mathcal{L}_{Dep(\widetilde{\mathcal{T}})}(\theta_F, \theta_D) + \sum_{i=1}^{N-1}(\mathcal{L}_{Dep(\widehat{\mathcal{T}}_i)}(\theta_F, \theta_D))) \quad (7)$$

Note that in (6), regression losses of depth estimation provides auxiliary supervision in the optimization of feature extractor. This can regularize the feature learning process of the feature extractor. In this way, the classifications in (1) and (3) within the meta learner are restrictively conducted in the feature space regularized by the auxiliary supervision of domain knowledge. This makes meta-train and meta-test focus on better-generalized learning directions.

Analysis. This section provides more detailed analysis on the proposed method. The objective of (5) in the meta-optimization is as follows (omitting θ_F for simplicity):

$$\min_{\theta_M} \sum_{i=1}^{N-1}(\mathcal{L}_{Cls(\widehat{\mathcal{T}}_i)}(\theta_M) + \mathcal{L}_{Cls(\widetilde{\mathcal{T}})}(\theta_{M_i}')) \quad (8)$$

$$f(x+h) = f(x) + h * f'(x)$$

We do the first-order Taylor expansion on the second term as follows:

$$\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_{M_i}{}') = \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_M)) =$$

$$\underbrace{\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M)}_{x} + \underbrace{\nabla_{\theta_M}\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M)^T}_{f'(x)} \underbrace{(-\alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_M))}_{h} \quad (9)$$

and the objective becomes:

(minimize loss in all meta-train & meta-test domains)

$$\min_{\theta_M} \sum_{i=1}^{N-1} (\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_M) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M)$$

→co-ordinate grad. info. btw meta train & test

$$- \alpha(\nabla_{\theta_M}\mathcal{L}_{Cls(\hat{\mathcal{T}}_i)}(\theta_M)^T \cdot \nabla_{\theta_M}\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M))) \quad (10)$$

to avoid overfitting to a single domain

The above objective shows that meta-optimization finds the generalized learning direction in the meta learner through: 1) minimizing losses in all meta-train and meta-test domains 2) meanwhile coordinating the learning directions (gradients information) between meta-train and meta-test so that the optimization can be conducted without overfitting to a single domain. It should be noted that there are two major differences compared to vanilla meta-learning for DG: 1) the above objective is conducted in feature space regularized by the domain knowledge supervision instead of in instance space (Li et al. 2018a). This makes both meta-train and meta-test focus on better-generalized learning directions and thus their learning directions are more likely to be coordinated in the task of face anti-spoofing (in the above third term). 2) vanilla meta-learning for DG (Li et al. 2018a) is simply conducted between one aggregated meta-train domain and one aggregated meta-test domain in each iteration. Comparatively, the above objective is simultaneously conducted between multiple $(N-1)$ pairs of meta-train and meta-test domains in each iteration. This adopts a fine-grained learning strategy that meta-learning is simultaneously conducted in a variety of domain shift scenarios in each iteration. Thus our face anti-spoofing model can be trained to generalize well to unseen attacks of various scenarios in each iteration.

Experiments

Datasets

The evaluation of our method is conducted on four public face anti-spoofing datasets that contain both print and video replay attacks: Oulu-NPU (Boulkenafet and et al 2017) (O for short), CASIA-MFSD (Zhang and et al 2012) (C for short), Idiap Replay-Attack (Chingovska, Anjos, and Marcel 2012) (I for short), and MSU-MFSD (Wen, Han, and Jain 2015) (M for short). Table 1 in the supplementary material[1] shows the variations in these four datasets. Figure 1 in the supplementary material shows some samples of the genuine faces and attacks. Table 1 and Fig. 1 in supplementary material show that compared to the seen training data, attacks from unseen materials, illumination, background, resolution and so on cause significant domain shifts among these datasets.

---

[1]Codes are available at https://github.com/rshaojimmy/AAAI2020-RFMetaFAS

Experimental Setting

Following the setting in (Shao et al. 2019), one dataset is treated as one domain in our experiment. We randomly select three datasets in four as source domains where domain generalization is conducted. The left one is the unseen domain for testing, which is unavailable in the training process. Half Total Error Rate (HTER) (Bengio and Mariéthoz 2004) (half of the summation of false acceptance rate and false rejection rate) and Area Under Curve (AUC) are used as the evaluation metrics in our experiments.

Implementation Details

Network Structure. Our deep network is implemented on the platform of PyTorch. The detailed structure of the proposed network is illustrated in Table 2 in the supplementary material. **Training Details.** The Adam optimizer (Kingma and Ba 2014) is used for the optimization. The learning rates α, β are set as 1e-3. The batch size is 20 per domain, and thus 60 for 3 training domains totally. **Testing.** For a new testing sample x, its classification score l is calculated for testing as follows: $l = M(F(x))$, where F and M are the trained feature extractor and meta learner.

Experimental Comparison

Baseline Methods. We compare several state-of-the-art face anti-spoofing methods as follows: **Multi-Scale LBP (MS_LBP)** (Määttä, Hadid, and Pietikäinen 2011) ; **Binary CNN** (Yang, Lei, and Li. 2014); **Image Distortion Analysis (IDA)** (Wen, Han, and Jain 2015); **Color Texture (CT)** (Boulkenafet, Komulainen, and Hadid 2016); **LBP-TOP** (Pereira and et al 2014); **Auxiliary** (Liu, Jourabloo, and Liu 2018): To fairly compare our method only using one frame information, we implement its face depth estimation component(denoted as Auxiliary(Depth Only)). We also compare its reported results (denoted as Auxiliary(All)); **MMD-AAE** (Li et al. 2018b); and **MADDG** (Shao et al. 2019). Moreover, we also compare the related state-of-the-art meta-learning for DG methods in the face anti-spoofing task: **MLDG** (Li et al. 2018a); **Reptile** (Nichol, Achiam, and Schulman. 2018); and **MetaReg** (Balaji and et al 2018).

Comparison Results. From comparison results in Table 1 and Fig. 4, it can be seen that the proposed method outperforms the state-of-the-art face anti-spoofing methods (Määttä, Hadid, and Pietikäinen 2011; Yang, Lei, and Li. 2014; Wen, Han, and Jain 2015; Boulkenafet, Komulainen, and Hadid 2016; Liu, Jourabloo, and Liu 2018). This is because all these methods focus on extracting differentiation cues the only fit to attacks in the source domains. Comparatively, the proposed meta-learning for DG trains our face anti-spoofing model to generalize well in the simulated domain shift scenario. This significantly improves the generalization ability of the face anti-spoofing method. Moreover, we also compare the DG with adversarial learning methods for face anti-spoofing (Li et al. 2018b; Shao et al. 2019) and our method also performs better. This is because instead of focusing on learning a domain shared feature space and training extra domain discriminators, our
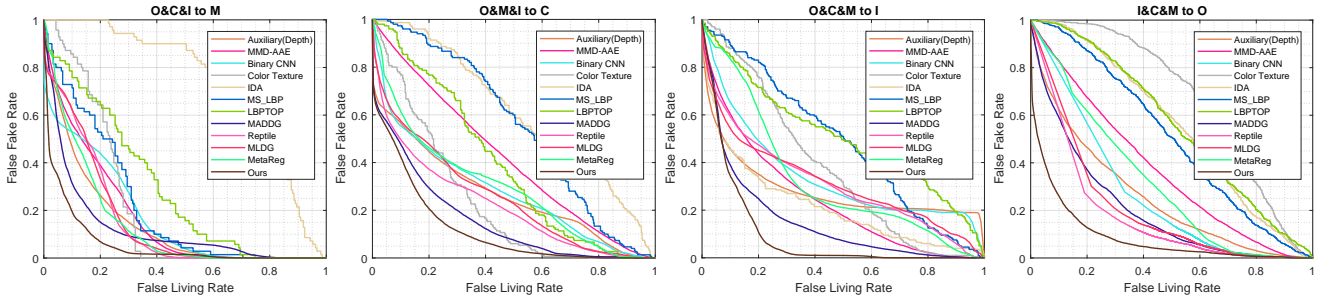
Figure 4: ROC curves of four testing sets for domain generalization on face anti-spoofing.

Table 1: Comparison to face anti-spoofing methods on four testing sets for domain generalization on face anti-spoofing.

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
MS_LBP	29.76	78.50	54.28	44.98	50.30	51.64	50.29	49.31
Binary CNN	29.25	82.87	34.88	71.94	34.47	65.88	29.61	77.54
IDA	66.67	27.86	55.17	39.05	28.35	78.25	54.20	44.59
Color Texture	28.09	78.47	30.58	76.89	40.40	62.78	63.59	32.71
LBPTOP	36.90	70.80	42.60	61.05	49.45	49.54	53.15	44.09
Auxiliary(Depth Only)	22.72	85.88	33.52	73.15	29.14	71.69	30.17	77.61
Auxiliary(All)	–	–	28.4	–	27.6	–	–	–
MMD-AAE	27.08	83.19	44.59	58.29	31.58	75.18	40.98	63.08
MADDG	17.69	88.06	24.5	84.51	22.19	84.99	27.98	80.02
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

Table 2: Comparison to meta-learning for DG methods on four testing sets for domain generalization on face anti-spoofing.

Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
Reptile	23.64	85.06	30.38	78.10	36.13	69.01	22.88	82.22
MLDG	23.91	84.81	32.75	74.51	36.55	68.54	25.75	79.52
MetaReg	21.17	86.11	35.66	70.83	32.28	67.48	37.72	68.71
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

method just needs to train a simple network with meta-learning strategy. This realizes the DG for face anti-spoofing in a more feasible and efficient way.

Table 2 and Fig. 4 show that compared to some state-of-the-art vanilla meta-learning for DG methods (Li et al. 2018a; Nichol, Achiam, and Schulman. 2018), our method also outperforms them for the task of face anti-spoofing. This illustrates that by addressing the above two issues, the proposed meta-learning framework is more able to improve the generalization ability for the task of face anti-spoofing.
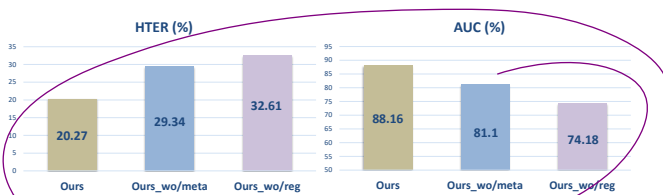
Ablation Study

Figure 5: Evaluation of different components of proposed method in O&M&I to C set for face anti-spoofing.

Components Evaluation. Considering that O&M&I to C set has the most significant domain shift, we evaluate different components of our method in this set for an example and experimental results are shown in Fig. 5. **Ours** denotes the proposed method. **Ours_wo/meta** denotes the proposed network without the meta-learning component. In this setting, we do not conduct the meta-learning in the meta learner part. **Ours_wo/reg** denotes the proposed network without domain knowledge regularization. In this setting, we do not incorporate the face depth maps as the domain knowledge to regularize the meta-learning process.

Figure 5 shows that the proposed network has degraded performance if any component is excluded. Specifically, the results of **Ours_wo/meta** verify that the meta-learning conducted in the meta learner benefits for the generalization ability improvement. The results of **Ours_wo/reg** show that without the regularization of domain knowledge supervision, the performance of our meta-learning for DG degrades significantly. This validates that by addressing the first issue, the proposed meta-learning framework is more able to develop a generalized face anti-spoofing model.

Table 3: Effectiveness of fine-grained learning strategy and second-order derivative information

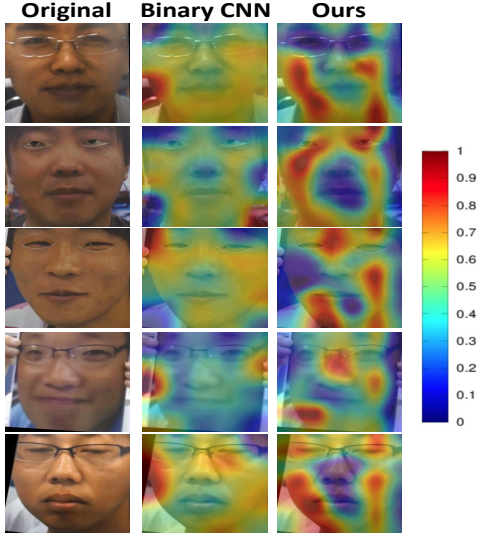| Method	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)	HTER(%)	AUC(%)
Ours (Aggregation)	14.54	92.87	24.28	85.29	20.07	88.13	17.94	90.69
Ours (First-order)	17.93	87.36	27.47	82.17	26.24	79.32	19.24	87.82
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

Figure 6: Attention map visualization of Binary CNN and our method for testing samples of attacks in O&M&I to C set. (Best reviewed in colors)

Effectiveness of fine-grained learning strategy and second-order derivative information. As mentioned in the above analysis, compared to vanilla meta-learning for DG methods, our method adopts a fine-grained learning strategy which can help to develop face anti-spoofing model with the generalization ability to unseen attacks of various scenarios. To verify the effectiveness of this strategy, we conduct our method in the setting proposed in (Li et al. 2018a), where the proposed regularized meta-learning is only conducted between one aggregated meta-train and one aggregated meta-test domains in each training iteration. The comparison results are named as Ours (aggregation) in Table 3. Table 3 shows that our method obtains better performance than Ours (aggregation). This validates that the proposed meta-learning adopting fine-grained learning strategy is more able to improve the generalization ability for the task of face anti-spoofing. Moreover, the third term in (10) has the function of coordinating the learning of meta-train and meta-test so as to prevent the optimization process from overfitting to a single domain. This improves the generalization ability but at the same time involves the second-order derivative computation of parameters of meta learner. Some works such as Reptile (Nichol, Achiam, and Schulman. 2018) uses a first-order approximation to decrease the computation complexity. We thus compare a method named as Ours (First-order) in Table 3 that replaces the second-order derivative computation in meta learner with the first-order approximation proposed in Reptile (Nichol, Achiam, and Schulman. 2018). Results show that our method performs better, which verifies that the second-order derivative information in the third term of (10) is more effective and plays a key role in the generalization ability improvement for the task of face anti-spoofing.

Attention Map Visualization

To provide more insights on why our method improves the generalization ability for the task of face anti-spoofing, we visualize the attention map of networks by the Global Average Pooling (GAP) method (Zhou et al. 2016). Figure 6 shows some examples of visualization results for the testing samples of attacks between Binary CNN (Yang, Lei, and Li. 2014) and our method. In (Yang, Lei, and Li. 2014), authors train a CNN only with supervision of binary class labels in the face anti-spoofing task. This makes the model focus on capturing biased differentiation cues with poor generalization ability. In the visualization of Binary CNN of Fig. 6, it can be seen that when encountering unseen testing attacks, this method pays the most attention to extracting the differentiation cues in the background (row 1-2) or on paper edges/holding fingers (row 3-5). These differentiation cues are not generalized because they will be changed if the attacks are from a new background or without clear paper edges. Comparatively, Fig. 6 shows that our method always focuses on the region of internal face for searching differentiation cues. These differentiation cues are more likely to be intrinsic and generalized for face anti-spoofing and thus the generalization ability of our method can be improved.

Conclusion

To improve the generalization ability of face anti-spoofing methods, this paper casts face anti-spoofing as a domain generalization problem, which is addressed in a new regularized fine-grained meta-learning framework. The proposed framework conducts meta-learning in the feature space regularized by the domain knowledge supervision. In this way, better-generalized learning information for face anti-spoofing can be meta-learned. Besides, a fine-grained learning strategy is adopted which enables a variety of domain shift scenarios to be simultaneously exploited for meta-learning so that our model can be trained to generalize well to unseen attacks of various scenarios. Comprehensive experimental results validate the effectiveness of the proposed method statistically and visually.

References

Antonio, T., and Efros, A. A. 2011. Unbiased look at dataset bias. In *CVPR*.

Balaji, Y., and et al. 2018. Metareg: Towards domain generalization using meta-regularization. In *NIPS*.

Bengio, S., and Mariéthoz, J. 2004. A statistical significance test for person authentication. In *The Speaker and Language Recognition Workshop*.

Bhushan Damodaran, B.; Kellenberger, B.; and et al. 2018. Deepjdot: Deep joint distribution optimal transport for unsupervised domain adaptation. In *ECCV*.

Boulkenafet, Z., and et al. 2017. Oulu-npu: A mobile face presentation attack database with real-world variations. In *FG*.

Boulkenafet, Z.; Komulainen, J.; and Hadid, A. 2016. Face spoofing detection using colour texture analysis. In *IEEE TIFS, 11(8): 1818-1830*.

Bousmalis, K.; Silberman, N.; Dohan, D.; Erhan, D.; and Krishnan, D. 2017. Unsupervised pixel-level domain adaptation with generative adversarial networks. In *CVPR*.

Chen, Q.; Liu, Y.; Wang, Z.; Wassell, I.; and Chetty, K. 2018. Re-weighted adversarial adaptation network for unsupervised domain adaptation. In *CVPR*.

Chingovska, I.; Anjos, A.; and Marcel, S. 2012. On the effectiveness of local binary patterns in face anti-spoofing. In *BIOSIG*.

Feng, Y.; Wu, F.; Shao, X.; Wang, Y.; and Zhou, X. 2018. Joint 3D face reconstruction and dense alignment with position map regression network. In *ECCV*.

Finn, C.; Abbeel, P.; and Levine, S. 2017. Model-agnostic meta-learning for fast adaptation of deep networks. In *ICML*.

He, K.; Zhang, X.; Ren, S.; and Sun, J. 2016. Deep residual learning for image recognition. In *CVPR*.

Kingma, D. P., and Ba, J. 2014. Adam: A method for stochastic optimization. In *arXiv preprint arXiv:1412.6980*.

Lan, X.; Ye, M.; Shao, R.; Zhong, B.; Yuen, P. C.; and Zhou, H. 2019. Learning modality-consistency feature templates: A robust rgb-infrared tracking system. In *IEEE TIE, 66(12), 9887–9897*.

Li, D.; Yang, Y.; Z, S. Y.; and et al. 2018a. Learning to generalize: Meta-learning for domain generalization. In *AAAI*.

Li, H.; Pan, S. J.; Wang, S.; and Kot, A. C. 2018b. Domain generalization with adversarial feature learning. In *CVPR*.

Liu, S.; Yuen, P. C.; Zhang, S.; and Zhao, G. 2016. 3D mask face anti-spoofing with remote photoplethysmography. In *ECCV*.

Liu, Y.; Jourabloo, A.; and Liu, X. 2018. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In *CVPR*.

Liu, S.; Lan, X.; and Yuen, P. C. 2018. Remote photoplethysmography correspondence feature for 3D mask face presentation attack detection. In *ECCV*.

Määttä, J.; Hadid, A.; and Pietikäinen, M. 2011. Face spoofing detection from single images using micro-texture analysis. In *IJCB*.

Mancini, M.; Porzi, L.; Rota Bul, S.; Caputo, B.; and Ricci, E. 2018. Boosting domain adaptation by discovering latent domains. In *CVPR*.

Nichol, A.; Achiam, J.; and Schulman., J. 2018. On first-order meta-learning algorithms. In *arXiv preprint arXiv:1803.02999*.

Pereira, T. F., and et al. 2014. Face liveness detection using dynamic texture. In *EURASIP Journal on Image and Video Processing, (1): 1-15*.

Pinheiro, P. O. 2018. Unsupervised domain adaptation with similarity learning. In *CVPR*.

Saito, K.; Watanabe, K.; Ushiku, Y.; and Harada, T. 2018. Maximum classifier discrepancy for unsupervised domain adaptation. In *CVPR*.

Shao, R., and Lan, X. 2019. Adversarial auto-encoder for unsupervised deep domain adaptation. In *IET Image Processing*.

Shao, R.; Lan, X.; Li, J.; and Yuen, P. C. 2019. Multi-adversarial discriminative deep domain generalization for face presentation attack detection. In *CVPR*.

Shao, R.; Lan, X.; and Yuen, P. C. 2017. Deep convolutional dynamic texture learning with adaptive channel-discriminability for 3D mask face anti-spoofing. In *IJCB*.

Shao, R.; Lan, X.; and Yuen, P. C. 2018. Feature constrained by pixel: Hierarchical adversarial deep domain adaptation. In *ACM MM*.

Shao, R.; Lan, X.; and Yuen, P. C. 2019. Joint discriminative learning of deep dynamic textures for 3D mask face anti-spoofing. In *IEEE TIFS, 14(4): 923-938*.

Tzeng, E.; Hoffman, J.; Saenko, K.; and Darrell, T. 2017. Adversarial discriminative domain adaptation. In *CVPR*.

Volpi, R.; Morerio, P.; Savarese, S.; and Murino, V. 2018. Adversarial feature augmentation for unsupervised domain adaptation. In *CVPR*.

Wen, D.; Han, H.; and Jain, A. K. 2015. Face spoof detection with image distortion analysis. In *IEEE TIFS, 10(4): 746-761*.

Yang, J.; Lei, Z.; and Li., S. Z. 2014. Learn convolutional neural network for face anti-spoofing. In *arXiv preprint arXiv:1408.5601*.

Ye, M.; Li, J.; Ma, A. J.; Zheng, L.; and Yuen, P. C. 2019. Dynamic graph co-matching for unsupervised video-based person re-identification. In *IEEE TIP, 28(6), 2976–2990*.

Zhang, Z., and et al. 2012. A face antispoofing database with diverse attacks. In *ICB*.

Zhang, J.; Ding, Z.; Li, W.; and Ogunbona, P. 2018a. Importance weighted adversarial nets for partial domain adaptation. In *CVPR*.

Zhang, W.; Ouyang, W.; Li, W.; and Xu, D. 2018b. Collaborative and adversarial network for unsupervised domain adaptation. In *CVPR*.

Zhou, B.; Khosla, A.; Lapedriza, À.; Oliva, A.; and Torralba., A. 2016. Learning deep features for discriminative localization. In *CVPR*.

Supplementary Material

Datasets

Table 4: Comparison of four experimental datasets.

Dataset	Light variation	Complex background	Attack type	Display devices
C	No	Yes	Printed photo Cut photo Replayed video	iPad
I	Yes	Yes	Printed photo Display photo Replayed video	iPhone 3GS iPad
M	No	Yes	Printed photo Replayed video	iPad Air iPhone 5S
O	Yes	No	Printed photo Display photo Replayed video	Dell 1905FP Macbook Retina

The evaluation of our method is conducted on four public face anti-spoofing datasets that contain both print and video replay attacks: Oulu-NPU (Boulkenafet and et al 2017) (O for short), CASIA-MFSD (Zhang and et al 2012) (C for short), Idiap Replay-Attack (Chingovska, Anjos, and Marcel 2012) (I for short), and MSU-MFSD (Wen, Han, and Jain 2015) (M for short). From Table 4 and Fig. 7, it can be seen that many kinds of variations, due to the differences on materials, illumination, background, resolution and so on, exist across these four datasets. Therefore, significant domain shift exists among these datasets.

Network Structure

The detailed structure of the proposed network is illustrated in Table 5. To be specific, each convolutional layer in the feature extractor, meta learner and depth estimator is followed by a batch normalization layer and a rectified linear unit (ReLU) activation function, and all convolutional kernel size is 3×3. The size of input image is $256 \times 256 \times 6$, where we extract the RGB and HSV channels of each input image. Inspired by the residual network (He et al. 2016), we use a short-cut connection, which is concatenating the responses of pool1-1, pool1-2 and pool1-3, and sending them to conv3-1 for depth estimation. This operation helps to ease the training procedure.
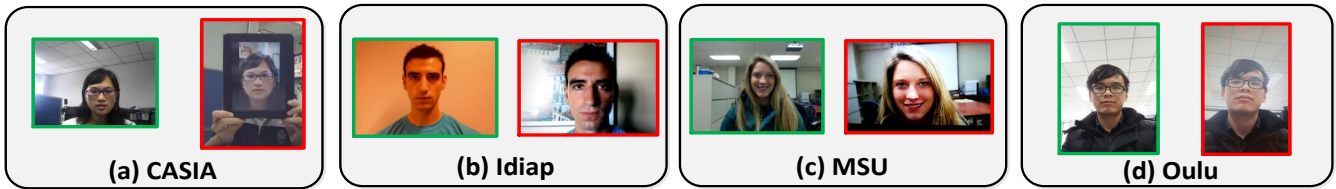
Figure 7: Sample frames from CASIA-MFSD (Zhang and et al 2012), Idiap Replay-Attack (Chingovska, Anjos, and Marcel 2012), MSU-MFSD (Wen, Han, and Jain 2015), and Oulu-NPU (Boulkenafet and et al 2017) datasets. The figures with green border represent the real faces, while the ones with red border represent the video replay attacks. From these examples, it can be seen that large cross-dataset variations due to the differences on materials, illumination, background, resolution and so on, cause significant domain shift among these datasets.

Table 5: The structure details of all components of the proposed network.

Feature Extractor			Meta Learner			Depth Estimator		
Layer	Chan./Stri.	Out.Size	Layer	Chan./Stri.	Outp.Size	Layer	Chan./Stri.	Outp.Size
Input			Input			Input		
image			pool1-3			pool1-1+pool1-2+pool1-3		
conv1-1	64/1	256	conv2-1	128/1	32	conv3-1	128/1	32
conv1-2	128/1	256	pool2-1	-/2	16	conv3-2	64/1	32
conv1-3	196/1	256	conv2-2	256/1	16	conv3-3	1/1	32
conv1-4	128/1	256	pool2-2	-/2	8			
pool1-1	-/2	128	conv2-2	512/1	8			
conv1-5	128/1	128	Average pooling					
conv1-6	196/1	128	fc2-1	1/1	1			
conv1-7	128/1	128						
pool1-2	-/2	64						
conv1-8	128/1	64						
conv1-9	196/1	64						
conv1-10	128/1	64						
pool1-3	-/2	32						