Journal of Computers Vol. 33 No. 5, October 2022, pp. 83-93
doi: 10.53106/199115992022103305008

A Domain Generalization Method Based on Hybrid Meta-Learning for Face Anti-Spoofing

Shuting Wei[1], Zhiyuan Shi[1], Zhibin Gao[2], Sheng Zhang[2], Lianfen Huang[2*]

[1] School of Electronic Science and Engineering, Xiamen University, Fujian 361102, China
weishuting@stu.xmu.edu.cn, zyshi@xmu.edu.cn
[2] School of Informatics, Xiamen University, Fujian 361005, China
gaozhibin@xmu.edu.cn, zhangsheng@stu.xmu.edu.cn, lfhuang@xmu.edu.cn

Received 5 December 2021; Revised 2 February 2022; Accepted 2 March 2022

Abstract. For face anti-spoofing, many methods have been proposed to improve the security of face recognition systems. Due to distribution discrepancies among different domains, it is difficult to seek a generalized space which can generalize well to unseen attacks. In this paper, we propose a framework based on meta-learning method to improve the generalization ability of face anti-spoofing. The feature extractor is trained with forcing the distribution of real faces more compact while the distribution of fake faces is more dispersed among domains. Then we add a hybrid-domain meta learner module to simulate multiple domain shift scenarios. Moreover, we add a refined triplet mining to constrain the distance between real faces and fake ones. Multiple gradient information is integrated to optimize the feature extractor and train the model with good generalization performance to unseen attacks of various scenarios. Extensive experiments on four public datasets show that our proposed method can get better generalization ability to unseen target domain compared with state-of-the-art methods.

Keywords: face anti-spoofing, domain generalization, meta-learning

1 Introduction

As one of the computer vision techniques, face recognition has become a critical choice in various security applications and it is widely used in real life, such as smartphones payment, border control and automated teller machine (ATM). While bringing convenience to people's life, face recognition technology also has many problems. As the reproduction of face is very easy to achieve, many types of presentation attacks (PA) for face recognition systems also appear. There are three main types of attacks that increase security risks: print face photos (print attack), replaying a face on a digital device (replay attack), the three-dimensional mask (3D-mask attack). Therefore, face anti-spoofing has become an increasingly critical role to cope with human face attacks and verify whether the detected face is true and reliable.

A variety of face anti-spoofing methods have been proposed. The traditional methods [1] utilize hand-craft feature to discriminate between the real faces and false faces because there is some unique texture information in the printed photos. With the development of deep learning, the methods of face anti-spoofing using CNN network is obviously more effective [2-6]. The face anti-spoofing methods based on CNN have obtained a lot of outstanding results, but they still have some problems in improving the performance when test on invisible test domains.

Due to domain discrepancy, only database-biased [7] features can be extracted when different distribution relationships of multiple domains are not considered, leading to poor generalization performance on unseen domains. To solve this problem, in recent years, many workers [8-12] begin to adopt domain adaptation techniques. These methods aim to transfer knowledge from labeled source domains to unseen target domains. Then, some researchers [2-3] explore domain generalization (DG) techniques, which assumes no access to any target data. Conventional DG methods learn a generalized feature space by aligning the distributions among various source domains. Then, some workers [4] propose that it is difficult to optimize by seeking a generalized feature space for the fake faces. Subsequently, some researchers [13-15] propose to explore DG technology in meta-learning framework. However, the generalization ability of DG methods for face anti-spoofing still needs to be improved. Most of them simulate a variety of actual shift scenarios in training and test process, but only use meta gradient for optimization. Besides, some of them use domain knowledge, leading to single optimization and complex pretreatment of data. To avoid such problems, we design a framework combined with a meta learner module, classifier and refined triplet mining to improve the performance of face anti-spoofing.

* Corresponding Author

In this paper, a domain generalization method combined with hybrid-domain meta-learning is proposed to improve the generalization ability, as shown in Fig. 1. We propose to conduct hybrid-domain meta-learning and learn a generalized feature space, forcing the feature distribution of real faces more compact and the fake ones more dispersed in the feature space, which generalizes better to the target domain. Suppose that we have N source domains, to simulate the shift scenarios from real faces to unseen domain, the meta-train conduct on the real faces in N-1 source domains and the remaining original domain is used as the meta-test domain. The refined triplet mining is added to aggregate the real faces of source domains while separate the fake faces. As a result, triplet loss, classifier loss and meta optimization jointly improve the generalization ability in training process. The main contributions of our method can be summarized as follows:

(1) An effective domain generalization framework combined with meta-learning method is proposed to improve the performance of face anti-spoofing.

(2) We learn a generalized feature space, where the feature distribution of real faces is compact while the feature distribution of fake faces is dispersed. A meta learner module is added behind the feature extractor to simulate multiple hybrid-domain shift scenarios. Moreover, we add the framework with refined triple mining to make real faces compact and make the distance between real faces and fake faces farther.

(3) We conduct experiments and comparisons based on four public datasets. Compared with several methods, the results show the effectiveness of proposed method.

The rest of the paper is organized as follows: in Section 2, we review the related work. In Section 3, we present the details of framework and introduce the proposed method. In Section 4, we present the experimental setup and evaluation of the proposed method on various tasks. Finally, we conclude our work in Section 5.

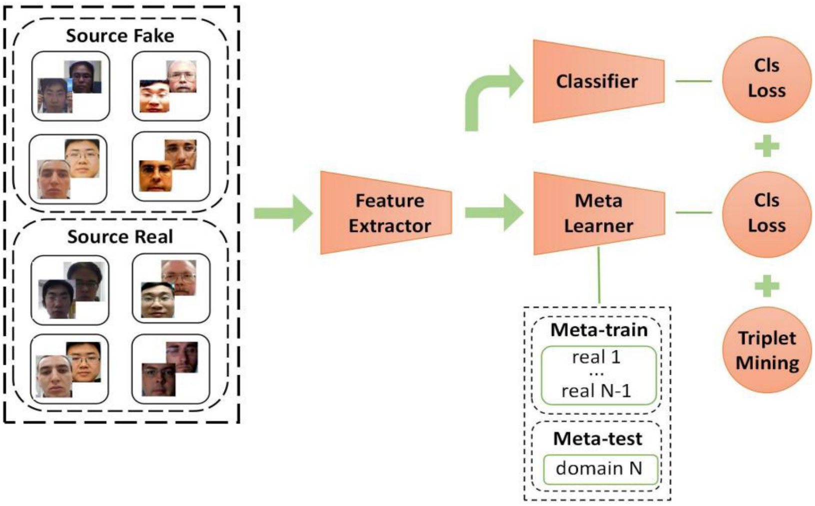

Fig. 1. Overview of proposed framework

2 Related Work

2.1 Face Anti-spoofing Methods

Face anti-spoofing plays an important role in face recognition, which has developed from methods using traditional methods to deep learning. Many traditional methods mainly use the difference between real and fake faces to design hand-craft feature. For example, some researchers [1] find that using chroma component and color texture analysis can improve performance for distinguishing. Freitas et al. [16] propose to combine spatial and temporal information into a descriptor. However, with the emergence of high-definition cameras and 3D masks, the better performance cannot be achieved by these traditional methods.

With the development of deep learning, the face anti-spoofing methods based on deep learning have outperformed traditional methods. Yang et al. [17] propose to use deep convolution neural network (CNN) to learn feature representation with high resolution under supervision to replace artificially designed features, significantly improving the performance of face anti-spoofing. Subsequently, there are many methods based on deep learning. Xu et al. [5] propose a CNN-LSTM architecture to extract temporal features for face anti- spoofing. Liu et al. [6] fuse the estimated depth information and rPPG signal as auxiliary supervision and propose a novel CNN-RNN network to distinguish between live and spoof faces. And Jourabloo et al. [18] propose a CNN architecture to decompose a spoof face into a spoof noise and a live face, and then utilize the spoof noise for classification. These methods significantly improve the performance and accuracy of face anti-spoofing, making it more robust and effective. However, most of these methods cannot solve the distribution discrepancies among different domains, leading to poor generalization performance on unseen domains.

2.2 Domain Generalization for Face Anti-spoofing

DG is still a challenging issue for face anti-spoofing problems. DG methods can generalize to unseen domains by learning the relationship between multiple source domains without accessing any target data. It was proposed by Blanchard et al. [19] as a machine learning problem in 2011. Holding the thought that the extracted features of the invisible domain can be mapped nearby the shared feature space, many researchers [2-3, 20] propose to learn the features with good robustness to the offset of target domain by aligning the feature distributions of source domains. Moreover, Jia et al. [4] propose that the attack types of fake faces are different in multiple domains, so it is difficult to optimize their generalized feature space. Thus, they train a feature extractor which makes only the real faces from different domains undistinguishable, but not for the fake ones. Their ideas of dividing the source domains into real faces and fake faces for feature extractor and forcing the distribution of real faces more compact can greatly improve the performance of domain generalization.

2.3 Meta-learning for Domain Generalization Methods

In view of the poor generalization ability to unseen domains of face anti-spoofing, meta-learning methods are proposed. The meta-learning methods aim to use the learned information to quickly adapt to the new tasks that have not been learned. Li et al. [13] and Finn et al. [14] propose to use agnostic model for meta-learning. Qin et al. [21] regard the face anti-spoofing problem as zero- and few-shot learning and propose adaptive inner-update meta face anti-spoofing (AIM-FAS) method. Most of them divide the source domains into two groups. In the meta-learning process, each iteration simulates a single domain shift scenario trough a meta-train domain and a meta-test domain to improve the generalization ability. In [15], Shao et al. propose to divide the source domains into multiple meta-train and meta-test domains, and conduct meta-learning between each pair of them in each iteration. In this way, various domains shift scenarios can be simulated at the same time and the model can learn to generalize well to unseen attacks.

3 Proposed Method

3.1 Overview

As shown in Fig. 1, we propose a domain generalization framework combined with a hybrid-domain meta learner module for face anti-spoofing. We seek a feature space with better generalization ability to unseen domains, choosing different optimization goals for the feature distributions of the real faces and fake ones. In addition, a refined triplet mining is added to constrain the distance between real faces and fake faces. In order to improve the generalization ability to unseen test domains, we propose to add a hybrid-domain meta learner module to simulate various domains shift scenarios during the training process. In conclusion, we use classifier, meta optimization and triplet loss to make the model learn to generalize well.

3.2 Feature Extractor

Since the attack types and collecting ways of fake faces are different while the real faces are extracted from real people, the distribution discrepancies among fake faces are larger than that the real faces. Learning a generalized feature space for both real and fake faces may lead to the poor generalization performance and be difficult to optimize. In our proposed method, we choose to learn a generalized feature space which has a compact distribution of real faces by forcing the features of real faces more compact while the features of fake faces disperse among different domains and compact within each domain. A feature classifier module is designed behind the feature extractor and the parameters of feature extractor are optimized by minimizing the loss of classifier loss and other objectives. Firstly, we separate the real faces from fake faces of the source domains and extract the features of them. Then we feed the features to the classifier to optimize the feature extractor and feed the source data to the meta learner to conduct meta-learning to improve the generalization ability. In order to further improve the performance, a refined triplet loss is added to aggregate the real faces and make the distance between real faces and fake faces farther.

3.3 Hybrid-domain Meta-learning

Since we adopt the thought that learning a generalized feature space which has a compact distribution of the real faces in multiple source domains and a disperse distribution of the fake faces among domains, we need to ensure that the model can generalize well to invisible domains. In order to achieve this goal, a meta learner module is added behind the feature extractor to conduct meta-learning. We define the parameter θ_F of feature extractor and θ_M of meta learner to optimize the model. For the meta learner module, we adopt hybrid-domain strategy. As shown in Fig. 2, supposing that there are N source domains, we randomly select N-1 source domains and sample the real faces from them as meta-train, and the remaining one as meta-test. In meta-test process, we simulate the domain shifts by assuming that the meta-test domain is the invisible test domain. With the above thoughts, the training can simulate the shift scenarios from real faces to unseen domain and this model can deal with a variety of attacks without any information of test domain. The algorithm of meta-learner model is shown in Algorithm 1.

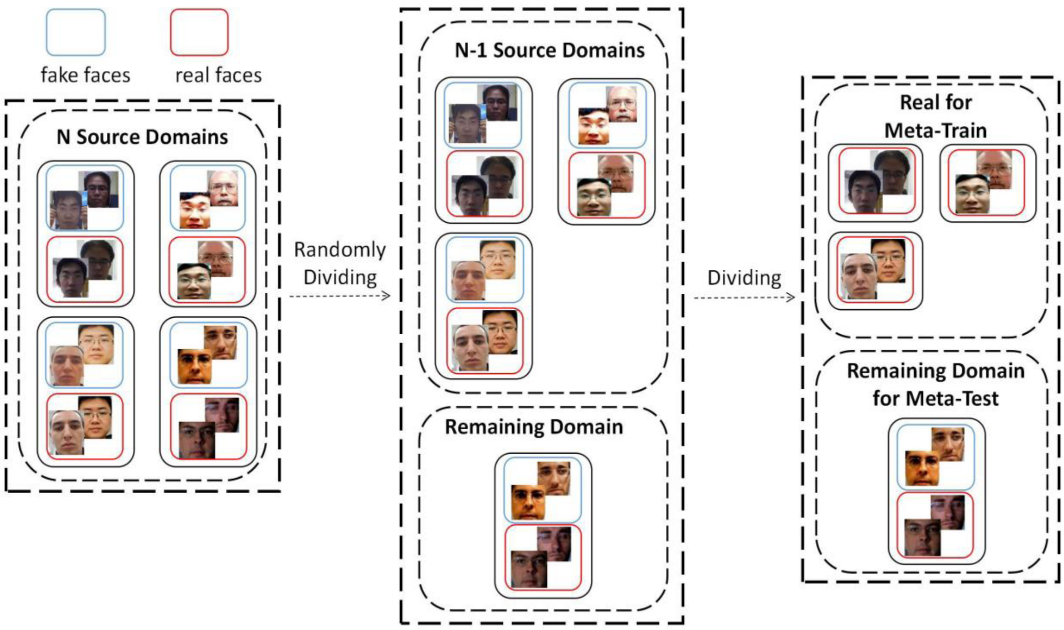

Fig. 2. Hybrid-domain strategy for meta-train and meta-test

Algorithm 1. Hybrid-domain Meta-learning

Input: Source domains $D = [D_1, D_2, ..., D_N]$
Init: Model parameters θ_F , θ_M.
Hyperparameters α , γ.
Randomly selecting N-1 source domains D as D_{mtr}
Selecting the remaining one source domain as D_{mte}
Meta-train:
Sampling real faces batch in each D_{mtr} as r_i ($i \in \{1, 2, ..., N-1\}$

for each of **do**

$L_{r_i}(\theta_F, \theta_M) = \sum_{(x,y)\epsilon r_i} ylogM\big(F(x)\big) + (1-y)\log\Big(1 - M\big(F(x)\big)\Big)$

$\theta'_{Mi} = \theta_M - \alpha\ _{\theta_M}L_{r_i}(\theta_F, \theta_M)$

end for

Meta-test:

Sampling batch in D_{mte} as Γ

$L_\tau(\theta_F, \theta_{M_i}') = \sum_{(x,y)\epsilon\tau} ylogM_i'(F(x)) + (1-y)log(1 - M_i'(F(x)))$

Meta-optimization:

update $\theta \leftarrow \theta - \gamma\nabla_\theta(\sum_{i=1}^{N-1}(L_{r_i}(\theta_F, \theta_M) + L_\tau(\theta_F, \theta_{M_i}')))$

end while

3.3.1 Meta-Train

In order to learn how to generalize well to unseen domain, we divide the datasets into meta-train sets and meta-test sets in meta learner. In our setting, we hope to learn the ability of transferring compact feature distribution of real faces to unseen domain. Therefore, assuming that there are N source domains, we randomly selecting N-1 source domains and sample real faces from them as meta-train domains. With the cross-entropy classification, the loss function [15] can be written as:

$$L_{r_i}(\theta_F, \theta_M) = \sum_{(x,y)\epsilon r_i} ylogM(F(x)) + (1-y)log(1 - M(F(x))) \ . \qquad (1)$$

where θ_F and θ_M are the parameters of the feature extractor and the meta learner, M and F stand for meta-learner and feature extractor component, respectively. We update the parameters with stochastic gradient descent:

$$\theta_{M_i}' = \theta_M - \alpha\nabla_{\theta_M} L_{r_i}(\theta_F, \theta_M) \ . \qquad (2)$$

The step size α can be fixed as a hyperparameter. For all meta-train batches, we sum the loss functions of each batch for the following meta-optimization.

3.3.2 Meta-Test

Since we aim to learn the generalized feature space which has compact feature distribution of real faces, we need to ensure that it can generalize well to the unseen test domain. In order to simulate the shift scenarios to unseen domain, we select the remaining source domain after meta-train and sample batch as the meta-test domain. In each meta-test evaluation, we regard the meta-test domain as unseen domain to simulate the attacks in various real scenarios. Then we update the parameters according to the loss function. Based on the updated meta learner parameters, we can get the loss function [15] for meta-test:

$$L_\tau(\theta_F, \theta_{M_i}') = \sum_{(x,y)\epsilon\tau} ylogM_i'(F(x)) + (1-y)log(1 - M_i'(F(x))) \ . \qquad (3)$$

where θ_{Mi}' is the parameter of updated meta learner. For all meta-test batches, we also sum the loss functions of each batch for meta-optimization.

3.3.3 Meta-Optimization

After meta-train and meta-test, we integrate all information for meta optimization:

$$L_{meta} = \sum_{i=1}^{N-1}(\beta_1 L_{r_i}(\theta_F, \theta_M) + \beta_2 L_\tau(\theta_F, \theta_{M_i}')) \ . \qquad (4)$$

The parameters are updated as follows:

$$\theta_F \leftarrow \theta_F - \gamma \nabla_{\theta_F}\left(\sum_{i=1}^{N-1}\left(L_{r_i}(\theta_F, \theta_M) + L_\tau(\theta_F, \theta_{M_i}')\right)\right) . \quad (5)$$

$$\theta_M \leftarrow \theta_M - \gamma \nabla_{\theta_M}\left(\sum_{i=1}^{N-1}\left(L_{r_i}(\theta_F, \theta_M) + L_\tau(\theta_F, \theta_{M_i}')\right)\right) . \quad (6)$$

3.3.4 Analysis

In this section, we discuss the main reasons why the meta learner can improve the generalization ability:

(1) The combination of meta-train and meta-test process simulates the multiple domain shift scenarios and coordinates the learning direction between meta-train and meta-test to conduct optimization without over-fitting to a single domain.

(2) Suppose that we have N source domains, in each iteration, the optimization is conducted on the *N*-1 meta-train domains and one meta-test domain, rather than simply performing the optimization iteration between single meta-train and meta-test domain.

(3) The meta-optimization function covers all meta-train and meta-test iterations at the same time so that multiple domain shift scenarios are considered simultaneously.

3.3 Triplet Mining

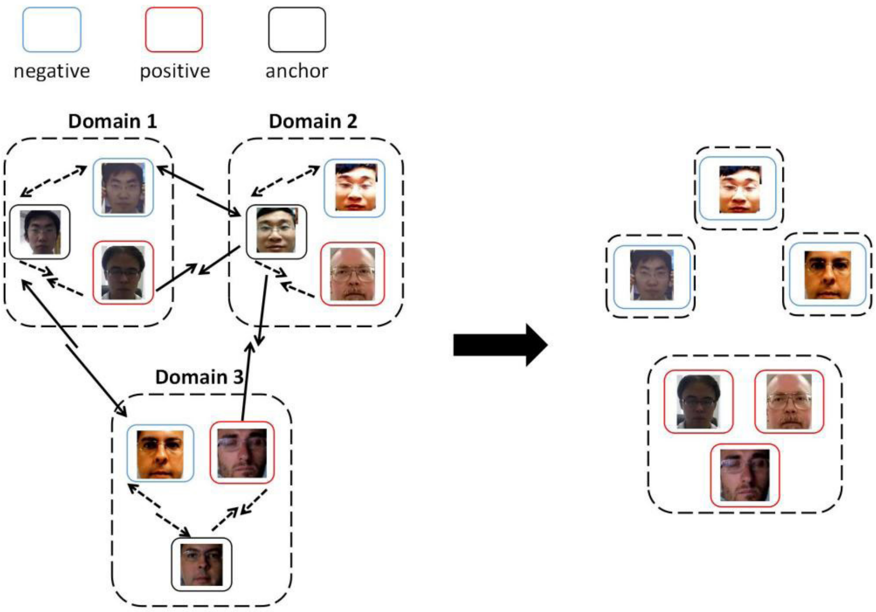

Fig. 3. Illustration of the triplet loss

As shown in Fig. 3, since we choose to learn a generalized space, where the feature distribution of real faces is compact while that of fake faces is dispersed among domains and compact within each domain, we need to make the real faces more compact in the feature space and make the fake faces more dispersed. In the meantime, we should not only aggregate real faces of all domains and pull apart the fake ones away from them, but also make the real faces in different domains more compact. In this way, we will learn a better and clear class boundary, getting a better performance for generalization. In our method, we use triplet loss [22] to reach this goal:

$$L_{TRI} = \min \sum_{x_i^a, x_i^p, x_i^n} (||f(x_i^a) - f(x_i^p)||_2^2 - ||f(x_i^a) - f(x_i^n)||_2^2 + \mu) . \quad (7)$$

where x_i^a, x_i^p, x_i^n denote the anchor, positive and negative samples, and α is a pre-defined margin. This loss function narrows down the distance between the anchor and positive samples and makes the distance between the anchor and negative samples farther.

Nong et al. [23] propose that when the distribution centers of different classes are dispersed, though the optimization may stagnate, we cannot ensure that the cluster of individual classes is compact enough. It means that in addition to making different clusters far away enough, we also need to make the anchor and positive examples compact enough. To this end, we add MSE to calculate the internal distance between anchor example and positive example:

$$L_{MSE} = \min \frac{1}{N} \sum_{i=1}^{N} (x_i^a - x_i^p)^2 \ . \quad \textbf{(8)}$$

The final loss includes the triplet mining loss function and MSE function, which can be represented as:

$$L_{Trip} = L_{TRI} + L_{MSE} \ . \quad \textbf{(9)}$$

3.4 Loss Function

As shown in the Fig. 1, We optimize the model with a meta-learner. A classifier is added behind the feature extractor and optimized with a standard cross entropy loss. With all loss functions above, the objective of proposed method is as follows:

$$LOSS = \lambda_1 L_{meta} + \lambda_2 L_{Trip} + \lambda_3 L_{cls} \ . \quad \textbf{(10)}$$

λ_1, λ_2, λ_3 are preset balance parameters. The generalization ability improvement of our method is good mainly through:

(1) We combine a variety of information in our model. The feature extractor is optimized by meta learner, classifier and refined triplet mining loss function.

(2) Following the hybrid-domain meta-learning strategy, the meta learner simulates multiple domain shift scenarios, finding the generalization learning direction through meta-train and meta-test. The meta-learning performs in multiple pairs of meta domains and coordinates the gradient information so as to get better generalization in the real scenarios.

(3) The refined triplet mining aims to separate the fake faces of different domains to force them to be more dispersed in the feature space and aggregate all the real faces to force them to be more compact, which helps us to learn a generalized feature space with good generalization ability.

4 Experiments

4.1 Datasets

We evaluate the effectiveness of our method on four public face anti-spoofing datasets as follows: Oulu-NPU [24] (denoted as O), CASIA-MFSD [25] (denoted as C), Idiap Replay-Attack [26] (denoted as I) and MSU-MFSD [27] (denoted as M).

4.2 Experimental Setting

To show the performance of domain generalization, we evaluate our method on four public databases. With randomly selecting three databases as the source domains and the remaining one as the target domain, we have four testing tasks in total: O&C&I to M, O&M&I to C, O&C&M to I and I&C&M to O. There exist many differences across these four databases, which exists multiple testing scenarios including intra-database and across-database among them. Half Total Error Rate (HTER) and Area Under Curve (AUC) are used as the evaluation metrics:

$$\mathrm{HTER} = \frac{\mathrm{FAR+FRR}}{\mathrm{FRR}} \ . \quad \textbf{(11)}$$

where FAR and FRR represents false acceptance rate and false rejection rate, respectively. We also present the Receiver Operating Characteristic (ROC) curves to further show the comparison results.

4.3. Implementation Details

Our framework is implemented by PyTorch. Following the work of [4], We use the feature extractor defined in ResNet-18 [28], replacing the last average pooling layer of ResNet-18 by the global pooling layer (GAP). And we add a fully connected layer (FC) as the bottleneck layer. The meta learner contains two convolutional blocks with average pooling layer and an FC layer at the end. The face anti-spoofing classifier is a simple linear model with a 2 nodes FC layer. As for optimization solver, we use SGD optimizer for the optimization. During training, all the input images are resized to 256×256×3. The learning rates in meta learner are set as 1e-3. The values of main parameters are shown in Table 1.

Table 1. Main parameters

Symbol	Value
β_1	0.5
β_2	0.5
μ	0.1
λ_1	1
λ_2	1
λ_3	0.5

4.4 Experimental Comparison

4.4.1 Ablation Experiment

To further evaluate the performance of each part, we evaluate different components of our method and the ablation experiments results are shown in Table 2. Ours denotes the proposed method. Ours w/o meta denotes the proposed model without the meta-learning component. In this task, we do not conduct the meta-learning process in the training. Ours w/o classifier denotes the designed model removing the classifier module. In this task, we do not incorporate the classification loss into the design. Similarly, Ours w/o triplet denotes the proposed model without triplet mining part. In this task, we do not use triplet mining to constrain the distance of faces in the learning process.

Table 2. Evaluation of different components of proposed method

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 w/o meta	11.429	94.333	16.667	91.141	20.571	80.512	19.566	88.588
Ours w/o classifier	42.857	60.289	36.222	67.686	27.143	75.915	40.382	64.585
Ours w/o triplet	14.524	92.537	19.889	87.730	19.286	85.198	18.056	90.035
Ours	10.000	96.422	16.000	90.684	16.286	88.466	15.538	92.381

As we can see in Table 2, the proposed model degrades performance if any component is excluded and adding all modules can obtain the best performance with the average HTER and AUC results are 14.46% and 91.99%, respectively. In the O&M&I to C experiment, the result of the AUC without meta learner is slightly better. Specifically, the results of Ours w/o classifier show that without the feature classifier, the performance of our method for DG degrades significantly. The results of Ours w/o meta verify that the hybrid-domain meta-learning strategy conducted in the meta learner is beneficial for the generalization ability improvement. Meanwhile, the results of Ours w/o triplet show that it is feasible to learn a generalized feature space with aggregating all the real faces from multiple domains. In summary, the classifier stabilizes the effectiveness of the whole framework and both of meta-learner and triplet mining can further improve the performance. The incorporation of all these components can achieve the best results.

4.4.2 Comparison with State-of-the-art Methods

In this part, we conduct several experiments to show the effectiveness of our proposed method. We compare our method with several state-of-the-art face anti-spoofing methods and meta-learning method for DG problem as follows: Multi-Scale LBP (MS-LBP) [29]; Binary CNN [17]; Image Distortion Analysis (IDA) [27]; Color Texture (CT) [1]; LBPTOP [30]; Auxiliary [6] and regularized fine-grained meta-learning [15] , we call it FGL for short.

Table 3. Comparison to state-of-the-art methods 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
CT	28.09	78.47	30.58	76.89	40.40	62.78	63.59	32.71
LBPTOP	36.90	70.80	33.52	73.15	29.14	71.69	30.17	77.61
Auxiliary (Depth)	22.72	85.88	33.52	73.15	29.14	71.69	30.17	77.61
Auxiliary (All)	-	-	28.40	-	27.60	-	-	-
MADDG	17.69	88.06	24.50	84.51	22.19	84.99	27.98	80.02
FGL	13.89	93.98	20.27	88.16	17.30	90.48	16.45	91.16
Ours	10.000	96.422	16.000	90.684	16.286	88.466	15.538	92.381

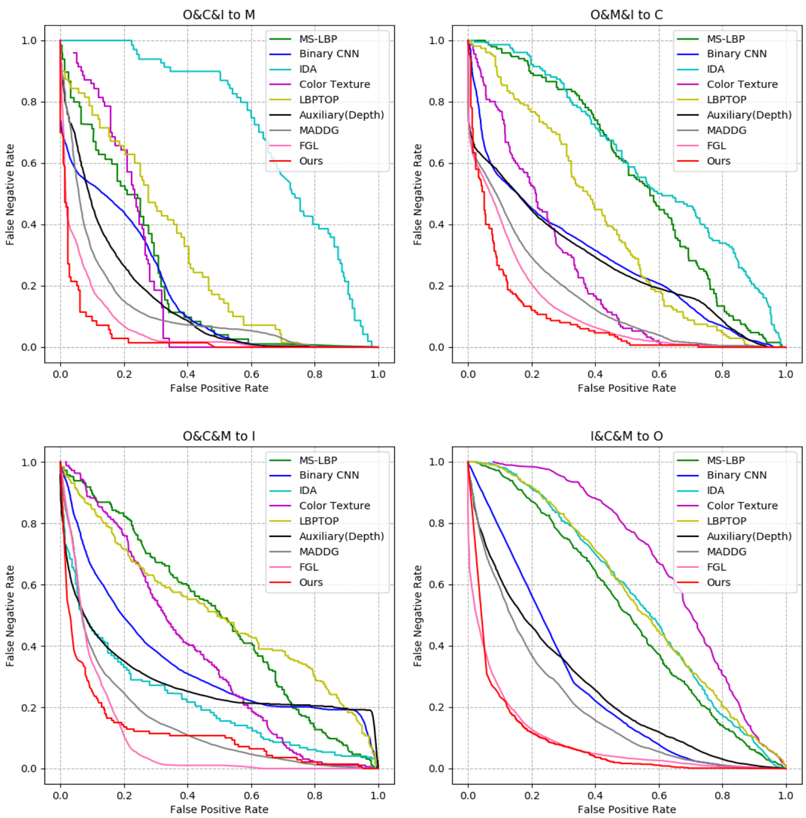

Fig. 4. ROC curves of four testing sets for domain generalization on face anti-spoofing

The HTER and AUC results of the comparison with other methods are shown in Table 3. And the ROC results of the comparison with state-of-the-art and meta methods are shown in Fig. 4. As shown in Table 3 and Fig. 4, we can find that the proposed method outperforms several face anti-spoofing methods, all HTER results are better than the method in [15] based on meta-learning though the AUC performance of O&C&M to I is not the best. For meta-learning, the average HTER results of FGL and us of all total testing tasks are 16.98% and 14.46%, respectively. The average AUC results of FGL and us of all total testing tasks are 90.95% and 91.99%, respectively. In comparison, these face anti-spoofing methods except MADDG do not consider different relationship between multiple source domains, extracting database biased features. Although MADDG method exploits the domain relationship of multiple source feature spaces, it chooses to learn a generalized feature space for real faces and fake faces, which cannot optimize easily and adapt to several attacks. The FGL method based on meta-learning has excellent performance by simulating multiple domain shift scenarios. Comparatively, our proposed method based on hybrid-domain meta-learning strategy performs better. We consider training feature extractor by multiple information at the same time instead of simply training with meta-learning strategy. For conclusion, it is effective for the face anti-spoofing task to combine the model with meta learner to improve generalization ability and train a feature extractor with forcing real faces more compact and constraining the distance of real faces and fake faces.

5 Conclusion

To improve the generalization ability of face anti-spoofing, this paper proposes a meta domain generalization method following a hybrid-domain meta-learning strategy. We follow the thought that learning a generalized feature space which has a compact distribution of real faces can get good generalization ability. Besides, we add a refined triplet mining to make the real faces more compact. Then the meta learner conducts meta-train and meta-test following hybrid-domain strategy, so as to simulate multiple domain shift scenarios. The final optimization function including refined triplet mining loss, classifier loss and the meta optimization is conducted to learn a generalized feature space. Extensive experiments show that our method is effective for improving generalization ability and achieves good results on four public databases. Future research will aim to further improve the performance of face anti-spoofing and explore other effective methods of face anti-spoofing.

6 Acknowledgement

The work presented in this paper was partially supported by National Natural Science Foundation of China (Grant number 61971365 and 61871339), 2021 University-Industry Collaborative Innovation Project of Fujian (2021H6001), and by Key Laboratory of Digital Fujian on IoT Communication, Architecture and Security Technology (Grant number 2010499)

References

[1] Z. Boulkenafet, J. Komulainen, A. Hadid, Face Spoofing Detection Using Colour Texture Analysis, IEEE Transactions on Information Forensics and Security 11(8)(2016) 1818-1830.
[2] H.-L. Li, S.J. Pan, S.-Q. Wang, A.C. Kot, Domain Generalization with Adversarial Feature Learning, in: Proc. 2018 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
[3] R. Shao, X.-Y. Lan, J.-W. Li, P.C. Yuen, Multi-Adversarial Discriminative Deep Domain Generalization for Face Presentation Attack Detection, in: Proc. 2019 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019.
[4] Y. Jia, J. Zhang, S.-G. Shan, X.-L. Chen, Single-Side Domain Generalization for Face Anti-Spoofing, in: Proc. 2020 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2020.
[5] Z.-Q. Xu, S. Li, W.-H. Deng, Learning Temporal Features using LSTM-CNN Architecture for Face Anti-Spoofing, in: Proc. 2015 3rd Asian Conference on Pattern Recognition (ACPR), 2015.
[6] Y. Liu, A. Jourabloo, X. Liu, Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision, in: Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
[7] A. Torralba, A.A. Efros, Unbiased Look at Dataset Bias, in: Proc. 2011 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2011.
[8] R. Shao, X.-Y. Lan, P.C. Yuen, Feature Constrained by Pixel: Hierarchical Adversarial Deep Domain Adaptation, in: Proc. 2018 ACM Multimedia Conference (MM'18), 2018.
[9] W.-C. Zhang, W.-L. Ouyang, W. Li, D. Xu, Collaborative and Adversarial Network for Unsupervised Domain Adaptation, in: Proc. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[10]P.O. Pinheiro, Unsupervised Domain Adaptation with Similarity Learning, in: Proc. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
[11]R. Volpi, P. Morerio, S. Savarese, V. Murino, Adversarial Feature Augmentation for Unsupervised Domain Adaptation, in: Proc. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
[12]J. Zhang, Z.-W. Ding, W.-Q. Li, P. Ogunbona, Importance Weighted Adversarial Nets for Partial Domain Adaptation, in: Proc. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
[13]D. Li, Y.-X. Yang, Y.-Z. Song, T.M. Hospedales, Learning to Generalize: Meta-Learning for Domain Generalization, in: Proc. 2017 Association for the Advancement of Artificial Intelligence (AAAI), 2017.
[14]C. Finn, P. Abbeel, S. Levine, Model-Agnostic Meta-Learning for Fast Adaptation of Deep Networks, in: Proc. 2017 International Conference on Machine Learning, 2017.
[15]R. Shao, X.-Y. Lan, P.C. Yuen, Regularized Fine-grained Meta Face Anti-spoofing, in: Proc. 2020 Association for the Advancement of Artificial Intelligence (AAAI), 2020.
[16]T. de Freitas Pereira, A. Anjos, J.M. De Martino, S. Marcel, LBP-TOP Based Countermeasure against Face Spoofing Attacks, in: Proc. 2012 Asian Conference on Computer Vision, 2012.
[17]J.-W. Yang, Z. Lei, S.-Z. Li, Learn Convolutional Neural Network for Face Anti-Spoofing. <https://arxiv.org/abs/1408.5601>, 2014 (accessed 15.10.21).
[18]A. Jourabloo, Y.-J. Liu, X.-M. Liu, Face De-Spoofing: Anti-Spoofing via Noise Modeling, in: Proc. 2018 European Conference on Computer Vision (ECCV), 2018.
[19]G. Blanchard, G. Lee, C. Scott, Generalizing from Several Related Classification Tasks to A New Unlabeled Sample, in: Proc. 2011 Neural Information Processing Systems, 2011.
[20]M. Ghifary, W.B. Kleijn, M. Zhang, D. Balduzzi, Domain Generalization for Object Recognition with Multi-task Autoencoders, in: Proc. 2015 IEEE International Conference on Computer Vision (ICCV), 2015.
[21]Y.-X. Qin, C.-X. Zhao, X.-Y. Zhu, Z.-Z. Wang, Z.-T. Yu, T.-Y. Fu, F. Zhou, J.-P. Shi, Z. Lei, Learning Meta Model for Zero- and Few-shot Face Anti-spoofing, in: Proc. 2020 Association for the Advancement of Artificial Intelligence (AAAI), 2020.
[22]F. Schroff, D. Kalenichenko, J. Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering, in: Proc. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.
[23]X.-Z. Nong, Y. Zeng, H.-F. Hu, Face Anti-Spoofing with Refined Triplet Loss and Multi-Level Attention Constraint Network, Electronics Letters 57(24)(2021) 912-914.
[24]Z. Boulkenafet, J. Komulainen, L. Li, X.-Y. Feng, A. Hadid, OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations, in: Proc. 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG), 2017.
[25]Z.-W. Zhang, J.-J. Yan, S.-F. Liu, Z. Lei, D. Yi, S.Z. Li, A face AntiSpoofing Database with Diverse Attacks, in: Proc. 2012 5th IAPR International Conference on Biometrics (ICB), 2012.
[26]I. Chingovska, A. Anjos, S. Marcel, On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing, in: Proc. 2012 International Conference of Biometrics Special Interest Group (BIOSIG), 2012.
[27]D. Wen, H. Han, A.K. Jain, Face Spoof Detection with Image Distortion Analysis, IEEE Transactions on Information Forensics and Security 10(4)(2015) 746-761.
[28]K. He, X. Zhang, S. Ren, J. Sun, Deep Residual Learning for Image Recognition, in: Proc. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.
[29]J. Määttä, A. Hadid, M. Pietikäinen, Face Spoofing Detection from Single Images using Micro-Texture Analysis, in: Proc. 2011 International Joint Conference on Biometrics (IJCB), 2011.
[30]T.D.F. Pereira, J. Komulainen, A. Anjos, J.M.D Martino, A. Hadid, M. Pietikainen, S. Marcel, Face Liveness Detection using Dynamic Texture, EURASIP Journal on Image and Video Processing 2014(2014) 2.