

# **A Survey of Domain Generalization-Based Face Anti-spoofing**

Fangling Jiang<sup>1</sup>, Yunfan Liu<sup>2</sup>, Bing Liu<sup>1</sup>, Xiaoliang Chen<sup>3</sup>, and Qi Li<sup>2( $\boxtimes$ )</sup>

<sup>1</sup> School of Computer Science, University of South China, Hengyang 421001, China jfl@usc.edu.cn <sup>2</sup> CRIPAC, NLPR, CASIA, Beijing 100190, China qli@nlpr.ia.ac.cn <sup>3</sup> SoundAI Technology Co., Ltd., Beijing 100190, China

Abstract. In recent years, remarkable research attention has been attracted to improve the generalization ability of face anti-spoofing methods, and domain generalization techniques have been widely exploited for adapting face anti-spoofing models to unseen testing scenarios. In this paper, we present a comprehensive survey on domain generalizationbased face anti-spoofing methods. Specifically, we propose a taxonomy for existing methods and conduct a thorough review on these methods by comparing and analyzing their motivations, highlights, and common technical characteristics. Afterward, we introduce commonly used datasets and evaluation metrics, and also analyze the performance of existing methods to uncover key factors affecting the generalization performance. Finally, we conclude this survey with a forecast on promising future research directions.

**Keywords:** Face anti-spoofing *·* Domain generalizaiton *·* Unseen testing scenarios *·* Generalied feature learning

### **1 Introduction**

With the rapidly growing application of face recognition systems in financial transaction and social security, face anti-spoofing, an important technique which aims to protect the identity verification process from presentation attacks, has been receiving increasing attention due to its theoretical significance and practical value. Most conventional face anti-spoofing methods, no matter based on hand-crafted features or spatial and temporal features learned with deep neural networks, assume that the training and testing data have identical and independent distributions (i.e., the *i.i.d.* assumption). However, this assumption does not hold in many practical applications of face anti-spoofing due to the large variation in image acquisition scenes, capturing devices, and manufacturing processes.

Intuitively, it is extremely difficult, if not impossible, to collect training data which could cover all possible variations of the potential presentation attack in real world applications, and thus the gap between the distribution of training and test data would always exist. Consequently, due to such data discrepancy, directly applying the decision boundary learned with training data to testing images, which are usually unavailable during training, would inevitably produce incorrect classification results and lead to a dramatic performance drop (see Fig.  $1(a)$  $1(a)$ ). Therefore, improving the generalization performance on unseen testing scenarios is critical for the development of practical face anti-spoofing methods.



<span id="page-1-0"></span>**Fig. 1.** Illustration of (a) the gap between the distribution of training and testing data, (b) problem definition of domain generalization-based face anti-spoofing. *P*(*X*) refers to the data distribution of domain *X*, and (c) explanation of all notations included.

As one of the most effective potential techniques for solving this problem, domain generalization [\[1](#page-8-0)] aims to learn a model that could be well-generalized to testing domains unseen during the training process from one or several different but related source domains. Since the goal of improving generalization performance on unseen testing scenarios is largely consistent with that of face anti-spoofing (see Fig.  $1(b)$  $1(b)$ ), domain generalization was first introduced to this field in [\[2\]](#page-8-1) and has been extensively explored in subsequent work, which is summarized in Table [1.](#page-2-0) Due to the remarkable breakthrough made and the great number of studies proposed in domain generalization-based face anti-spoofing, in this paper, we present a comprehensive survey of research in this field to summarize existing approaches and forecast promising future research directions. To the best of our knowledge, this is the first literature review of face anti-spoofing methods focusing on their generalization ability on unseen testing scenarios, where most previous surveys mainly center on discussing conventional methods that do not consider the domain discrepancy.

The rest of this article is organized as follows. In Sect. [2,](#page-2-1) we review existing methods in this field and present a taxonomy for systematic summarization and comparison. In Sect. [3,](#page-5-0) we introduce commonly used datasets and evaluation metrics, and also analyze the performance of existing methods to uncover important factors affecting the generalization performance. Afterward, we discuss potential research directions in Sect. [4,](#page-7-0) aiming to inspire more related work targeting the improvement of the generalization performance of face anti-spoofing in the future. Finally, we draw some conclusions in Sect. [5.](#page-8-2)

## <span id="page-2-1"></span>**2 Methodologies**

In this section, we review existing domain generalization-based face anti-spoofing methods in detail by comparing and analyzing their motivations, highlights, and common technical characteristics. Table [1](#page-2-0) gives an overview and a taxonomy of these methods. It is worth noting that all these methods are categorized according to their main innovations.

Category	Method	Year	Highlights			
Domain align- ment	$MLDG$ [2]	2018	Minimize the MMD distance			
	MADDG <sup>[3]</sup>	2019	Multi-adversarial shema, dual-force triplet mining constraint, depth constraint			
	DAF $[4]$	2020	Class-conditional domain discriminator module with a gradient reversal layer, temporal domain-invariant feature learning			
	$SSDG$ [5]	2020	Single-side adversarial learning, asymmetric triplet loss			
	DRDG <sup>[6]</sup>	2021	Sample and feature reweighting, depth constraint			
	SDFANet <sup>[7]</sup>	2021	Local-region and global image alignment, domain attention strategy, multi-scale attention fusion			
	$CDA$ [8]	2022	Conditional domain adversarial, parallel domain reg- ularization			
	$CSD-S$ [9]	2022	Single-side adversarial learning, asymmetric triplet loss, low-rank decomposition			
Meta-learning	<b>RFM</b> [10]	2020	Meta-learning regularized by depth constraint			
	$D^2$ AM [11]	2021	Pseudo domain labels			
	$FAS-DR-BC$ [12]	2021	Meta-teacher, bi-level optimization			
	PDL-FAS <sup>[13]</sup>	2021	Pseudo-domain labels, depth loss			
	$ANR$ [14]	2021	Adaptive feature normalization, inter-domain com- patible and inter-class separable loss			
	DBMNet [15]	2021	Two meta-learners regularized by a triplet loss and a depth loss, respectively			
	$HFN+MP$ [16]	2022	Learnable meta pattern extractor, bi-level meta opti- mization			
Disentangled representation learning	$DR-MD-Net$ [17]	2020	Disentangle liveness features from subject discrimi- native features			
	VLAD-VSA [18]	2021	Domain-shared and domain-specific visual words separation, centroid adaptation			
	$DASN$ [19]	2021	Suppress spoof-irrelevant factors, doubly adversarial learning			
	$SSAN$ [20]	2022	Content and style representation separation, enhance liveness-related style features and suppress domain- specific ones			
	Unknown Cam [21]	2022	Camera-invariant feature learning, feature decompo- sition, feature discrimination augmentation			
Data augmen- tation	$LMFD-PAD [22]$	2022	Learnable frequency filters, hierarchical attention module			
Physical cues supervision	$UAPG$ [23]	2020	Depth, material and reflection guided proxy tasks, uncertainty-aware attention			

<span id="page-2-0"></span>**Table 1.** Overview of domain generalization-based face anti-spoofing methods.

#### **2.1 Domain Alignment-Based Methods**

Most existing domain generalization-based face anti-spoofing methods fall into this category, where domain-invariant features are learned by minimizing the distribution discrepancies among source domains. Based on the specific technique adopted for aligning the source domains, these methods could be further divided into two sub-categories: maximum mean discrepancy minimizing based approaches and domain adversarial learning based approaches.

Li et al. [\[2](#page-8-1)] first introduce domain generalization to face anti-spoofing. They design a regularization term that minimizes the maximum mean discrepancy (MMD) distance among different domains to improve the generalization ability of learned features. Different from [\[2](#page-8-1)], most methods [\[3](#page-8-3)[–9,](#page-9-3)[19\]](#page-9-13) are based on the idea of domain adversarial learning [\[24](#page-9-18)]. Shao et al. [\[3](#page-8-3)] propose an adversarial learning scheme between a shared feature generator and multiple domain discriminators to align the marginal distributions among different domains and learn domain-invariant features. Considering the rich diversity of spoof face images, some work  $[4,5,8,9]$  $[4,5,8,9]$  $[4,5,8,9]$  $[4,5,8,9]$  $[4,5,8,9]$  proposes to handle the distribution of live and spoof face images in greater detail. Jia et al. [\[5\]](#page-9-0) align the distributions of live face images by single-side adversarial learning, and separate the spoof face images of each domain while aggregating the real ones of all domains by an asymmetric triplet loss. Low-rank decomposition is used to extend the work of [\[5\]](#page-9-0) to improve the robustness of the live and spoof face classifier in [\[9\]](#page-9-3). Furthermore, Jiang et al. [\[8](#page-9-2)] align the conditional distribution of both live and spoof faces from different domains to learn domain-invariant conditional features. Moreover, [\[6](#page-9-19),[7\]](#page-9-1) propose to perform refined feature alignments by giving different attention during domain adversarial training to samples, features, and regions of images.

Generally, features that are invariant to source domain shift could also be more generalized to the target domain. However, the generalization performance of existing methods on unseen target domains is still difficult to guarantee when the differences between the source-target and source-source domain shift are large. In face anti-spoofing, there are many factors that affect domain discrepancies, and the data on the current training set is usually limited, so this is a problem worthy of further study.

#### **2.2 Meta-Learning-Based Methods**

Meta-learning, which is known as learning-to-learn and aims to learn general knowledge from episodes sampled from related tasks, is a commonly used learning strategy to improve the generalization ability of models in domain generalization-based face anti-spoofing. Existing work has been studied from the aspects of feature learning  $[10,14,15]$  $[10,14,15]$  $[10,14,15]$  $[10,14,15]$ , supervision information  $[11-13]$  $[11-13]$  and input data [\[16](#page-9-10)].

From the perspective of feature learning, episodes are usually built according to unseen testing scenarios of face anti-spoofing. *M −* 1 of the *M* source domains are used as the meta-train set, and the remaining one is used as the meta-test set to simulate domain shift. After building episodes, Shao et al. [\[10](#page-9-4)]

and Jia et al. [\[15\]](#page-9-9) exploit a depth loss and a triplet loss to regularize the optimization process of meta-learners. Liu et al. [\[14](#page-9-8)] propose to adaptively select feature normalization methods to learn domain-invariant features. Considering domain labels usually are unknown in application, Chen et al. [\[11,](#page-9-5)[13\]](#page-9-7) generate pseudo-domain labels by feature clustering during meta-learning instead of using domain labels. Qin et al. [\[12](#page-9-6)] train a teacher to learn how to supervise the live and spoof classifier performing better rather than using handcrafted labels as supervision information. Besides, meta-learning is also used to construct a learnable network to automatically extract generalized input patterns for generalization performance improvement of face anti-spoofing [\[16](#page-9-10)].

#### **2.3 Disentangled Representation Learning-Based Methods**

It is a challenging task to force all learned features to be domain-invariant in face anti-spoofing due to the diversity of various influencing factors such as identities, spoof faces, acquisition environments, and acquisition devices. Intuitively, aligning part of all learned features that have a large impact on generalization performance and ignoring other features is a more feasible idea, and disentangled representation learning is an effective way to alleviate this problem. Disentangled representation learning-based face anti-spoofing methods generally decompose features into two parts: domain-shared features and domain-specific features, in which domain-shared features are encouraged to be domain-invariant and domain-specific features containing information about various influencing factors are suppressed.

Some work focuses on dealing with the negative impact of a single impact factor on generalization performance. The identity and camera discriminative features are disentangled from liveness features in [\[17](#page-9-11)] and [\[21](#page-9-15)] to improve the generalization ability of learned features. Other methods take into account a variety of spoof-irrelevant factors such as identity, acquisition environments, and acquisition devices. Kim et al. [\[19\]](#page-9-13) present a doubly adversarial learning framework to suppress these spoof-irrelevant factors and then enhance the generalization ability on unseen domains for face anti-spoofing. In [\[18\]](#page-9-12), the learned entire VLAD features are separated into domain-shared and domain-specific features, and only the domain-shared features are enforced to be domain-invariant. Besides, wang et al. [\[20](#page-9-14)] disentangle style features from content features, and design a contrastive learning loss to enhance liveness-related style features while suppressing the domain-specific ones.

#### **2.4 Others**

In addition to the above three categories, researchers have also tried to improve the generalization performance of face anti-spoofing from other perspectives. Fang et al. [\[22](#page-9-16)] extract frequency maps by learnable frequency filters as inputs from a data augmentation aspect. Physical cues such as depth, material, and reflection maps are used to supervise the face anti-spoofing model learning generalized features across domains in [\[23\]](#page-9-17).

Dataset	Year	Subjects	Samples	Acquisition Sce- narios	<b>Acquisition Devices</b>	<b>Presentation Attacks</b>	
$CASIA-$ MFSD [25]	2012	50	600	Indoor scenario	Low- and normal- quality USB cameras, high-quality Sony NEX-5 camera	Cut, warped, flat photos; Replayed videos (iPad)	
Replay- Attack [26]	2012	50	1200	Two illumina- tion conditions	Machook webcam	Printed $(Tri-$ photos umph Adler DCC 2520 color laser printer); Replayed photos and videos (iPhone 3GS, iPad)	
MSU- MFSD [27]	2015	35	280	Indoor scenario	Macbook air webcam, Nexus 5	Printed photos (HP Color Laserjet CP6015xh printer); Replayed videos (iPad Air, iPhone 5S)	
OULU- $NPU$ [28]	2017	55	5940	Three scenarios with back- ground and illumination variations	Frontal cameras of six types of smartphones	Printed photos (Canon image PRESS C6011, PIXMA iX6550 print- ers); Replayed videos (Dell UltraSharp) 1905FP, MacBook Retina)	

<span id="page-5-1"></span>**Table 2.** Commonly used datasets for domain generalization-based face anti-spoofing.

### <span id="page-5-0"></span>**3 Datasets and Evaluation**

**Datasets.** OULU-NPU, CASIA-MFSD, Replay-Attack, and MSU-MFSD are commonly used datasets in domain generalization-based face anti-spoofing. An overview of the characteristics of these datasets is provided in Table [2.](#page-5-1) It is clear that these datasets have large differences in acquisition devices, acquisition scenarios, and manufacturing processes of face artifacts, which causes the domain shift among different datasets and further brings challenges to the generalization of face anti-spoofing models. Most domain generalization-based face anti-spoofing methods follow the evaluation protocols in [\[3](#page-8-3)] for measuring the performance of benchmark approaches. These protocols are based on the idea of Leave-One-Out, where only one dataset is considered as the unseen target domain and the rest as source domains. Considering the high cost of building a dataset in face anti-spoofing, we hope to learn generalized models using as few source domains as possible. Therefore, the generalization ability of state-of-theart face anti-spoofing methods is also evaluated on limited source domains.

Although domain generalization-based face anti-spoofing has made great progress in recent years, there is still a gap between the academic experimental setting and the practical application environment, due to the difference in sample quantity and data distribution. To better simulate the practical application scenario, Costa-Paz et al. [\[20](#page-9-14)[,29](#page-10-2)] aggregate more than ten existing face antispoofing datasets together and design protocols in terms of acquisition devices, acquisition scenarios, and types of face artifacts to evaluate the generalization performance of face anti-spoofing models.

<span id="page-6-0"></span>

Year	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O		<b>AVG</b>
	<b>HTER</b>	AUC			<b>HTER</b>	AUC	<b>HTER</b>	<b>AUC</b>	<b>HTER</b>
		$(\% )$	$(\%)$	$(\%)$	$(\%)$	$(\%)$	$(\%)$	$(\%)$	$(\%)$
2018	23.91	84.81	32.75	74.51	36.55	68.54	25.75	79.52	29.74
2019	17.69	88.06	24.50	84.51	22.19	84.99	27.89	80.02	23.07
2020	17.02	90.10	19.68	87.43	20.87	86.72	25.02	81.47	20.65
2020	15.42	91.13	17.41	90.12	15.87	91.72	14.72	93.08	15.86
2020	13.89	93.98	20.27	88.16	17.30	90.48	16.45	91.16	16.98
2020	7.38	97.17	10.44	95.94	11.71	96.59	15.61	91.54	11.29
2021	15.40	91.80	24.50	84.40	15.60	90.10	23.10	84.30	19.65
2021	12.70	95.66	20.98	85.58	15.43	91.22	15.27	90.87	16.10
2021	12.43	95.81	19.05	88.79	15.56	91.79	15.63	91.75	15.67
2021	11.67	93.09	18.44	89.67	11.93	94.95	16.23	91.18	14.57
2021	10.83	96.75	17.85	89.26	16.03	91.04	15.67	91.90	15.10
2021	8.33	96.31	12.04	95.33	13.38	86.63	11.77	94.65	11.38
2021	7.86	96.54	14.00	94.58	16.42	90.88	17.59	90.92	13.97
2021	4.29	98.25	8.76	95.89	7.79	97.79	12.64	94.00	8.37
2021	4.28	97.59	12.56	93.63	6.14	97.30	12.26	94.29	8.81
2022	10.80	95.30	20.50	87.40	11.30	95.00	19.50	87.90	15.53
2022	10.48	94.55	12.50	94.17	18.49	84.72	12.41	94.95	13.47
2022	6.67	98.75	10.00	96.67	8.88	96.79	13.72	93.63	9.82
2022	6.19	97.90	10.20	94.87	16.00	89.59	13.33	93.66	11.43
2022	5.24	97.28	9.11	96.09	15.35	90.67	12.40	94.26	10.53
2022	5.00	97.58	10.00	96.85	12.07	94.68	13.45	94.43	10.13
		$(\%)$			<b>HTER</b> AUC				

<span id="page-6-1"></span>**Table 4.** Error Rate (%) of different types of unseen attacks on the protocol O&C&I to H, where 'H' represents the HQ-WMCA [\[32\]](#page-10-5) dataset, and 'O', 'C', and 'I' are abbreviations for OULU-NPU, CASIA-MFSD, and Replay-Attack, respectively.



**Evaluation Metrics.** Most existing methods are both qualitatively and quantitatively evaluated based on previously mentioned protocols. Commonly used quantitative evaluation metrics are Area Under Curve (AUC) ratio and Half Total Error Rate (HTER) [\[26](#page-9-21)], where HTER is the average of False Rejection Rate (FRR) and False Acceptance Rate (FAR). Some visualization tools such as t-SNE [\[33](#page-10-6)] and Grad-CAM [\[34\]](#page-10-7) are used to explore the decision-making process of the learned model and qualitatively measure the overall performances.

**Performance Analysis.** To uncover the important factors affecting the generalization performance of face anti-spoofing models, we conduct extensive experiments on existing methods on four protocols and throughly analyze their performance (shown in Table [3\)](#page-6-0). Generally, over the course of four years, the generalization performance has been significantly improved on all four protocols, although there is still plenty of room for continuous improvement.

Each of the four datasets in the protocols has its own characteristics. In consequence, the domain shift among the four protocols is different. According to Table [3,](#page-6-0) the state-of-the-art performance for each protocol is achieved by different methods. In other words, existing methods are still incapable of learning completely domain-invariance features for mitigating the gap between domains, and the difference between source-source and source-target domain shift is an important factor affecting the generalization performance. For instance, we regard HQ-WMCA as the target domain and focus on evaluating the impact of domain shift caused by unseen presentation attack instruments. The comparison results on the protocol  $O\&C\&I$  to H are shown in Table [4.](#page-6-1) Although SSDG-R18 achieves a lower HTER in the protocol  $O\&C\&I$  to M, the model learned from source domains O&C&I still has extremely high error rates for most types of unseen attacks from the HQ-WMCA dataset. Open set domain generalization could be an effective way to solve this problem.



<span id="page-7-1"></span>**Fig. 2.** Performance comparison among different types of methods.

Moreover, we could also conclude that the reduction of source domains leads to a sharp decline in performance. This indicates that both the scale and diversity of training data are important for improving the generalization performance of face anti-spoofing. Relatively speaking, disentangled representation learning and domain alignment-based methods achieve better overall performance than other categories of methods, as shown in Fig. [2.](#page-7-1) This indicates that suppressing domain-specific features and finely enforcing domain-shared ones to be domaininvariant is an effective way to improve the generalization ability for face antispoofing.

### <span id="page-7-0"></span>**4 Future Research Directions**

Though lots of efforts have been made on domain generalization-based face antispoofing as surveyed, there still remain many open problems. Here we summarize some challenges and future research directions in this field.

1) **Small-scale dataset.** Most existing face anti-spoofing datasets are small in scale and have limited diversity in the patterns of presentation attacks, and collecting a large-scale dataset covering diverse live and spoof face

images is extremely difficult and prohibitively expensive. However, it has been proved that finetuning models trained on large-scale datasets to downstream tasks can improve the generalization ability, and thus large-scale pretraining, self-supervised, semi-supervised, and few-shot domain generalization are worth investigating for face anti-spoofing. Besides, learning to generate novel domains to increase the diversity of source domains would be a promising direction.

- 2) **Interpretability.** Face anti-spoofing methods are usually used in scenarios with high-security requirements, but we still lack an understanding of learned features and the decision-making behavior of models. Exploring interpretable domain generalization-based face anti-spoofing methods is an urgent need for practical applications of face anti-spoofing.
- 3) **Heterogeneous approaches.** As shown in Sect. [3,](#page-5-0) most evaluation protocols currently are homogeneous. The source-source domain shift and sourcetarget domain shift are similar. In practical applications, the unseen target domain is unpredictable. The source-target domain shift may be large different from the source-source one. It would be interesting to see more work on datasets, evaluation protocols, and algorithms for heterogeneous domain generalization-based face anti-spoofing.

## <span id="page-8-2"></span>**5 Conclusion**

In this paper, we present a comprehensive survey on existing studies in domain generalization-based face anti-spoofing. Specifically, the problem definition, techniques, datasets, evaluation metrics, performance analysis, and future research directions are discussed in detail. We hope this survey could provide a valuable summarization for researchers who are interested in face anti-spoofing and inspire more future work to promote the development of this field.

**Acknowledgments.** This work is funded by the Beijing Municipal Natural Science Foundation (Grant No. 4222054), the Natural Science Foundation of Hunan Province (Grant No. 2022JJ30481), the Natural Science Foundation of China (Grant No. 62076240).

### **References**

- <span id="page-8-0"></span>1. Wang, J., Lan, C., Liu, C., Ouyang, Y., Qin, T.: Generalizing to unseen domains: a survey on domain generalization, arXiv preprint [arXiv:2103.03097](http://arxiv.org/abs/2103.03097) (2021)
- <span id="page-8-1"></span>2. Li, H., He, P., Wang, S., Rocha, A., Jiang, X., Kot, A.C.: Learning generalized deep feature representation for face anti-spoofing. TIFS **13**(10), 2639–2652 (2018)
- <span id="page-8-3"></span>3. Shao, R., Lan, X., Li, J., Yuen, P.C.: Multi-adversarial discriminative deep domain generalization for face presentation attack detection. In: CVPR, pp. 10023–10031 (2019)
- <span id="page-8-4"></span>4. Saha, S., et al.: Domain agnostic feature learning for image and video based face anti-spoofing. In: CVPR Workshops, pp. 802–803 (2020)
- <span id="page-9-0"></span>5. Jia, Y., Zhang, J., Shan, S., Chen, X.: Single-side domain generalization for face anti-spoofing. In: CVPR, pp. 8484–8493 (2020)
- <span id="page-9-19"></span>6. Liu, S., et al.: Dual reweighting domain generalization for face presentation attack detection, arXiv preprint [arXiv:2106.16128](http://arxiv.org/abs/2106.16128) (2021)
- <span id="page-9-1"></span>7. Zhou, L., Luo, J., Gao, X., Li, W., Lei, B., Leng, J.: Selective domain-invariant feature alignment network for face anti-spoofing. TIFS **16**, 5352–5365 (2021)
- <span id="page-9-2"></span>8. Jiang, F., Li, Q., Liu, P., Zhou, X., Sun, Z.: Adversarial learning domain-invariant conditional features for robust face anti-spoofing, arXiv preprint [arXiv:2205.22027](http://arxiv.org/abs/2205.22027) (2022)
- <span id="page-9-3"></span>9. Liu, M., Mu, J., Yu, Z., Ruan, K., Shu, B., Yang, J.: Adversarial learning and decomposition-based domain generalization for face anti-spoofing. PRL **155**, 171– 177 (2022)
- <span id="page-9-4"></span>10. Shao, R., Lan, X., Yuen, P.C.: Regularized fine-grained meta face anti-spoofing. In: AAAI, vol. 34, no. 07, pp. 11974–11981 (2020)
- <span id="page-9-5"></span>11. Chen, Z., et al.: Generalizable representation learning for mixture domain face anti-spoofing, arXiv preprint [arXiv:2105.02453](http://arxiv.org/abs/2105.02453) (2021)
- <span id="page-9-6"></span>12. Qin, Y., Yu, Z., Yan, L., Wang, Z., Zhao, C., Lei, Z.: Meta-teacher for face antispoofing. TPAMI (2021)
- <span id="page-9-7"></span>13. Kim, Y.E., Lee, S.-W.: Domain generalization with pseudo-domain label for face anti-spoofing, arXiv preprint [arXiv:2107.06552](http://arxiv.org/abs/2107.06552) (2021)
- <span id="page-9-8"></span>14. Liu, S., et al.: Adaptive normalized representation learning for generalizable face anti-spoofing. In: ACM MM, pp. 1469–1477 (2021)
- <span id="page-9-9"></span>15. Jia, Y., Zhang, J., Shan, S.: Dual-branch meta-learning network with distribution alignment for face anti-spoofing. TIFS **17**, 138–151 (2021)
- <span id="page-9-10"></span>16. Cai, R., Li, Z., Wan, R., Li, H., Hu, Y., Kot, A.C.: Learning meta pattern for face anti-spoofing. TIFS **17**, 1201–1213 (2022)
- <span id="page-9-11"></span>17. Wang, G., Han, H., Shan, S., Chen, X.: Cross-domain face presentation attack detection via multi-domain disentangled representation learning. In: CVPR, pp. 6678–6687 (2020)
- <span id="page-9-12"></span>18. Wang, J., et al.: VLAD-VSA: cross-domain face presentation attack detection with vocabulary separation and adaptation. In: ACM MM, pp. 1497–1506 (2021)
- <span id="page-9-13"></span>19. Kim, T., Kim, Y.: Suppressing spoof-irrelevant factors for domain-agnostic face anti-spoofing. IEEE Access **9**, 86966–86974 (2021)
- <span id="page-9-14"></span>20. Wang, Z., et al.: Domain generalization via shuffled style assembly for face antispoofing, arXiv preprint [arXiv:2203.05340](http://arxiv.org/abs/2203.05340) (2022)
- <span id="page-9-15"></span>21. Chen, B., Yang, W., Li, H., Wang, S., Kwong, S.: Camera invariant feature learning for generalized face anti-spoofing. TIFS **16**, 2477–2492 (2021)
- <span id="page-9-16"></span>22. Fang, M., Damer, N., Kirchbuchner, F., Kuijper, A.: Learnable multi-level frequency decomposition and hierarchical attention mechanism for generalized face presentation attack detection. In: WACV, pp. 3722–3731 (2022)
- <span id="page-9-17"></span>23. Wu, J., Yu, X., Liu, B., Wang, Z., Chandraker, M.: Uncertainty-aware physicallyguided proxy tasks for unseen domain face anti-spoofing, arXiv preprint [arXiv:2011.14054](http://arxiv.org/abs/2011.14054) (2020)
- <span id="page-9-18"></span>24. Ganin, Y., Lempitsky, V.: Unsupervised domain adaptation by backpropagation. In: International Conference on Machine Learning. PMLR, pp. 1180–1189 (2015)
- <span id="page-9-20"></span>25. Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., Li, S.Z.: A face antispoofing database with diverse attacks. In: ICB, pp. 26–31 (2012)
- <span id="page-9-21"></span>26. Chingovska, I., Anjos, A., Marcel, S.: On the effectiveness of local binary patterns in face anti-spoofing. In: International Conference of Biometrics Special Interest Group, pp. 1–7 (2012)
- <span id="page-10-0"></span>27. Wen, D., Han, H., Jain, A.K.: Face spoof detection with image distortion analysis. TIFS **10**(4), 746–761 (2015)
- <span id="page-10-1"></span>28. Boulkenafet, Z., Komulainen, J., Li, L., Feng, X., Hadid, A.: OULU-NPU: a mobile face presentation attack database with real-world variations. In: FG, pp. 612–618 (2017)
- <span id="page-10-2"></span>29. Costa-Pazo, A., Jiménez-Cabello, D., Vázquez-Fernández, E., Alba-Castro, J.L., López-Sastre, R.J.: Generalized presentation attack detection: a face anti-spoofing evaluation proposal. In: ICB, pp. 1–8 (2019)
- <span id="page-10-3"></span>30. Wang, J., Zhang, J., Bian, Y., Cai, Y., Wang, C., Pu, S.: Self-domain adaptation for face anti-spoofing, arXiv preprint [arXiv:2102.12129](http://arxiv.org/abs/2102.12129) (2021)
- <span id="page-10-4"></span>31. Kim, Y.-E., Nam, W.-J., Min, K., Lee, S.-W.: Style-guided domain adaptation for face presentation attack detection, arXiv preprint [arXiv:2203.14565](http://arxiv.org/abs/2203.14565) (2022)
- <span id="page-10-5"></span>32. Heusch, G., George, A., Geissbühler, D., Mostaani, Z., Marcel, S.: Deep models and shortwave infrared information to detect face presentation attacks. TBIOM **2**(4), 399–409 (2020)
- <span id="page-10-6"></span>33. Van der Maaten, L., Hinton, G.: Visualizing data using t-SNE. JMLR **9**, 2579–2605 (2008)
- <span id="page-10-7"></span>34. Selvaraju, R.R., Cogswell, M., Das, A., Vedantam, R., Parikh, D., Batra, D.: Gradcam: visual explanations from deep networks via gradient-based localization. In: ICCV, pp. 618–626 (2017)