Unsupervised Progressive Learning Approach for Cross-Domain Iris Presentation Attack Detection

Hao-Liang Wen, Kuo-Chun Lin, and Yen-Ming Chen, *Member, IEEE*

***Abstract*—In the context of the proliferation of large-scale iris recognition systems globally, the necessity for efficient detection of visual attack images, such as textured contact lenses and printouts, has seen a marked increase. Existing methods for presentation attack detection (PAD) tend to struggle with generalization in invisible scenarios due to the unavailability of labeled training data in a novel domain.**

Addressing this issue, we suggest a semi-supervised domain adaptation methodology designed to facilitate the generalization of PAD across both seen and unseen data. The architecture comprises a classifier coupled with two generative adversarial networks (GANs). The classifier is designed to learn to generalize unseen features from the generative networks by amalgamating features derived from both labeled and unlabeled data. Each generative model caters to different labels - authentic or fraudulent, the choice of which is determined by the accuracy of the labeled data and the current prediction of unlabeled data.

Our proposed methodology adopts an end-to-end self-learning paradigm, enabling the system to learn and generalize both authentic and deceptive iris classifications. This approach has shown encouraging results when tested with the iris PAD databases from the LivDet-iris 2017 competitions.

***Index Terms*—Iris presentation attack detection, iris liveness detection, iris anti-spoofing, adversarial domain adaptation, progressive learning, iterative data process.**

I. Introduction

NUMEROUS biometric features have sprung up and sometimes fade as the field advances, but the recognition of the iris is a biometric trait that will certainly withstand the test of time. The iris pattern is unique and epigenetically determined by random events in the morphogenesis of this tissue[1], and thus offers high discrimination power, making it useful to distinguish even identical twins [2].

The robustness of iris recognition systems has been shown over time to be affordable, noninvasive, and touchless; However, these methods may become less reliable if their strengths allow them to grow in the market in the coming years [3]. Most iris recognition systems are based on near-infrared (NIR) lighting and sensors, and have been shown to be susceptible to presentation attack instruments (PAI) [4], where PAI refers to a biometric characteristic or object used in a presentation attack. The power and speed of the iris recognition system have propelled itself into large-scale applications, for example, Unique ID in India [5][6], and the NEXUS system operated jointly by the Canada Border Services Agency and US Customs and Border Protection to speed up the identification of prescreened travelers [7]. As iris recognition becomes more widespread, the number and variety of attempted attacks naturally increase as the number and variety of attacks increases, and the presentation-attack detection (PAD) problem has become an essential research topic.

According to the standardized vocabulary in ISO/IEC 30107-1, a presentation attack is a presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system[8].

Researchers and vendors from the biometric community have faced the challenge of proposing and developing efficient protection mechanisms against the threat [9], where PAD methods have been suggested as a solution to this vulnerability. Attacks are no longer restricted to merely theoretical or academic scenarios, as they are starting to be carried out against real-life operations. An example is the hacking of Samsung Galaxy S8 devices with the iris unlock system, using a regular printer and a contact lens. This case has been reported to the public from hacking groups attempting to obtain recognition for real criminal cases, as is noted in live biometric demonstrations at conferences1. An ideal PAD technique should be able to detect all these attacks, along with any new or unknown PAI species that may be developed in the future [4].

The Iris Liveness Detection Competition (LivDet-Iris, www.livdet.org) began in 2013[10]. This competition focuses on proper measurement of the ability of current technology to withstand presentation attacks that use artifacts, providing important insight into the pace of evolution of modern iris PAD methods. LivDet 2017 is the most recent competition with available training data. The results reported in the 2017 competition show that iris PAD algorithms are still far from achieving acceptable detection rates. Furthermore, LivDet's 2017 results suggest that challenging evaluation protocols such as interdata set and intersensor setups, hereinafter referred to as cross-domains, can be seen as a major limitation of the current PAD algorithms and current open research problem.

In recent years, cross-domain problems have been highlighted by several investigations [11]-[12]. It is pointed out by Agarwal et al. that cross-sensor and cross-dataset

Kuo-Chun Lin is with Institute of Communications Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan (e-mail: jimmy910259@gmail.com).

Yen-Ming Chen (Corresponding Author) is with Institute of Communications Engineering and Department of Electrical Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan (e-mail: emerychen.cm@gmail.com).

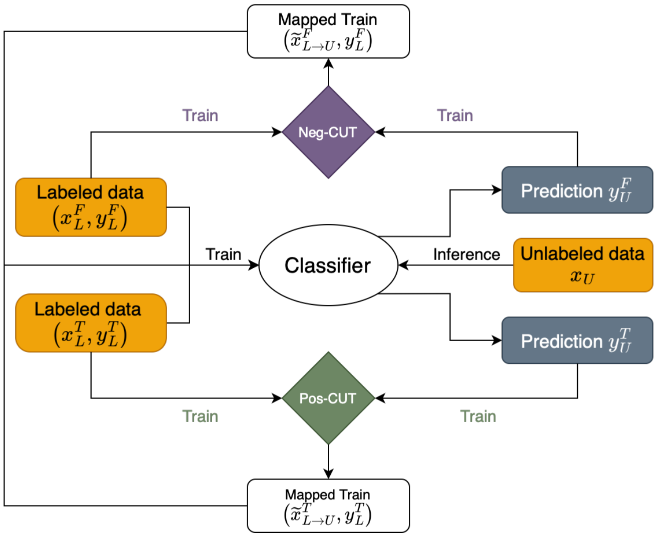

Figure 1: Flow chart of the proposed method. Two GAN networks are responsible for different labels from inference results. Synthetic data are generated by mapping training distributions to testing distributions using the corresponding GAN network.

issues are very important issues for real-world applications. Additionally, existing PAD methods have worse performance in cross-dataset settings than intra-dataset settings, indicating its inability to generalize well to unknown types of attacks [13]. Furthermore, a lower error rate is observed in cross-sensor settings than in cross-dataset settings. Some researchers considered the IIITD-WVU LivDet subset (IIITD-WVU dataset) as a cross-dataset evaluation because IIITD databases were used for training and a other test database captured at WVU using a mobile iris sensor and provided satisfactory accuracy in the results. However, the IIITD-WVU dataset does not generalize all kinds of attacks; we suppose this is the reason why the authors in [14] claimed that training CNN predictors in one data set and testing them in another resulted in accuracy no better than random predictions, even though they have shown some promising results in the IIITD-WVU dataset. To our knowledge, there are only a few papers [15][16] that deal with the challenges of cross-dataset deployments up to present. The authors report the evaluations with different dataset between training and testing datasets; however, there is still room for improvement.

To address cross domain issues, domain adaptation (DA) has been utilized to mitigate the gap between the target domain and the source domain for face PAD [17][18] and iris PAD [16] problems. In this paper, we are aimed to improve the PAD generalization ability for cross-domain problems by a semi-supervised learning approach. We leverage the unlabeled images from target domain and the labeled data in the source domains to build a PAD model that can generalize well to the target domain. To achieve this goal, a classifier is trained from the labeled source domain, then the classifier is adapted to the unlabeled target domain by training GAN models which obtain the robust ability to transform the images from the source domain to target domain. Eventually, the model achieves generalization ability through labeled data and the augmented data. The proposed approach is end-to-end trainable, and achieves promising results in cross-database iris PAD on several public-available datasets.

The main contributions of this work are three-fold: (i) a novel unlabeled domain adaptation approach that is able to leverage labeled source domain data and unlabeled target domain data to build robust PAD model; (ii) Progressive learning for obtaining domain independent features during domain adaptation; and (iii) promising PAD performance in a number of cross-database tests than the state-of-the-art approaches addressing generalized iris PAD.

Essential improvements in this work include: (i) we propose a iterative and augmented learning, which allows more domain independent knowledge to be transferred and used for distinguishing live vs. spoof iris images in the unlabeled target domain; (ii) we provide extensive evaluations using three datasets in public domain, e.g., Clarkson, Notre Dame, and IIITD-WVU datasets, and provide comparisons with several baselines for PAD, such as PBS [15], A-PBS [15], FAM+FMM [16]; and (iii) we have provided more details about our method implementation, experimental evaluation, and related work.

The remainder of this paper is organized as follows. Some preliminaries are presented in Section II, including basic concepts used in this work. Section III introduces the system model and the preliminaries outlining image preprocessing. Sections IV and V elaborate on the proposed EC-IR scheme based on the devised soft feature extraction strategy. In Section VI, the DFP-based EC-IR scheme is further proposed. Finally, Section VII concludes this paper.

II. Related Work

A. IRIS PAD

Daugman [19] proposed the first countermeasure for iris presentation attacks detection. Daugmans concepts include searching abnormality in Fourier spectrum to detect printed irises on a paper or contact lenses, detection of specular reflections from both the cornea and the lenses, or investigating pupil size variations. Thalheim et al. [20] have shown the first successful demonstration of impersonation with the utilize of a commercial sensor. They successfully attack on a commercial iris recognition system with authentic eyes previously enrolled by using iris images printed on a paper. Al-Raisi et al. [21] have presented the first use of ones eye to evade recognition observed in an operational environment was recorded at the border crossing point employing iris recognition in the United Arab Emirates. With the inspiration of these early demonstrations of vulnerabilities, other presentation attack instruments have been studied, including use of textured contact lenses that partially occlude the actual iris texture [22], presentation of iris images displayed on a screen [23], or use of prosthetic eyes [24] and the cadaver eyes [25].

Multiple PAD methods for iris recognition systems have been proposed in the scientific literature, given the increased adoption of these systems for a variety of different operations, which increases the threats of attacks on these sensitive systems. The hand-crafted approaches use various image descriptors to calculate image features, which are used to distinguish between authentic irises and artifacts, typically through the use of Support Vector Machine classifiers. Popular techniques used in the calculation of PAD-related iris image features are Binarized Statistical Image Features (BSIF) [26], Local Binary Patterns (LBP) [22], Binary Gabor Patterns (BGP) [27], Local Contrast-Phase Descriptor (LCPD) [28], Local Phase Quantization (LPQ) [29], Scale Invariant Descriptor (SID) [30], Scale Invariant Feature Transform (SIFT) and DAISY [31], Locally Uniform Comparison Image Descriptor (LUCID) and CENsus TRansform hISTogram (CENTRIST) [32], Weber Local Descriptor (WLD) [28], Wavelet Packet Transform (WPT) [33] or image quality descriptors proposed by Galbally et al. [34].

One may also benefit from recently popular data-driven approaches that learn directly from the data how to process and classify iris images to solve the PAD task [31], [35][36]. In [37], Zou et al. have presented a algorithm of 4DCycle-GAN for expanding spoofed iris image databases, by synthesizing artificial iris images wearing textured contact lenses. This method helps to create and increase the number of images based on conditional GANs while preserving the information in the images of each PAI in the NIR spectrum. In [38], domain-specific knowledge of iris PAD is incorporated into the design of their model (DACNN). With the domain knowledge, a compact network architecture is obtained, and regularization terms are added to the loss function to enforce high-pass/low-pass behavior. The authors demonstrate that the method can detect both face and iris presentation attacks. SpoofNets [39] are based on GoogleNet, and consist of four convolutional layers and one inception module. Boyd et al. [40] chose the ResNet50 architecture as a backbone to explore whether iris-specific feature extractors perform better than models trained for non-iris tasks. Nguyen et al. [41] proposed a PAD method by combining features extracted from local and global iris regions. Kuehlkamp et al. [14] propose an approach for combining two techniques for iris PAD: CNNs and Ensemble Learning.

B. Domain Adaptation for IRIS PAD

Domain adaptation (DA) aims to transfer the knowledge or model learned from a source domain to a target domain [42]. DA can be very useful when there is only limited training data in a new application scenario, and thus has received increasing attention in recent years [43].

Long et al. [44] proposed a Deep Adaptation Network (DAN) to map deep features into Reproducing Kernel Hilbert Spaces (RKHS). Then, they performed DA by minimizing the maximum mean discrepancy (MMD) [45]. Muhammad et al. [46] proposed a deep reconstruction-classification network (DRCN) to learn a common representation for both domains through the joint objective of supervised classification of labeled source data and unsupervised reconstruction of unlabeled target data. A number of approaches have utilized adversarial learning proposed in Generative Adversarial Networks (GANs) [47] to reduce the source and target domain discrepancy for better DA [48]-[49].

Domain adaptation (DA) techniques have been introduced to face anti-spoofing [50]-[51]. However, it has not been employed in iris PAD field yet until this year. Li et al. [16] proposed the first DA technique for iris PAD approach. They mix low frequency components of images from target domain with high frequency components of images from source domain through discrete cosine transform (DCT), in order to generate new samples with labels and styles of target domain. Nonetheless, this method do not fully exploit the useful information from the images of target domain. On one hand, it cannot gurrentee the transformation of the feature of the images between two domains comprehensive for the reason it only mix the original images with the low-frequency feature of the images from target domain, on the other hand, as the bonafide and attack images under the target domain are undistinguishable, it may induce a situation that bonafide images under the source domain are mixed with the attack images and make uncorrectable mistakes of training.

C. Contrastive Learning

Contrastive learning aims at learning an embedding representation space by maximizing similarity and dissimilarity on positive and negative data pairs, which has been extensively used in the metric learning [52] and self-supervised learning (SSL)[53], [54]. In the SSL setting, where the supervised information of training data is unavailable, contrastive learning focuses on learning an invariant representation space by designing various pretext tasks based on data transformations (e.g. rotation cropping and color-jittering) [53], [54].

Recently, Khosla et al. [55] have extended the contrastive loss for supervised training. Due to the exploration of local semantic structures, it is able to learn more powerful representations. As contrastive learning has achieved impressive results in representation learning, we believe it performs well in transformation of cross-domain images. Concretely, since the supervision of the target domain is unavailable, it fails to bridge the two domains directly and immediately. Thus, unlike the way for the construction of paired data in SSL, the domain-adaptive prototypes are utilized in our progressive learning method to serve as category anchors, guiding the construction of contrastive pairs in feature space for contrastive learning.

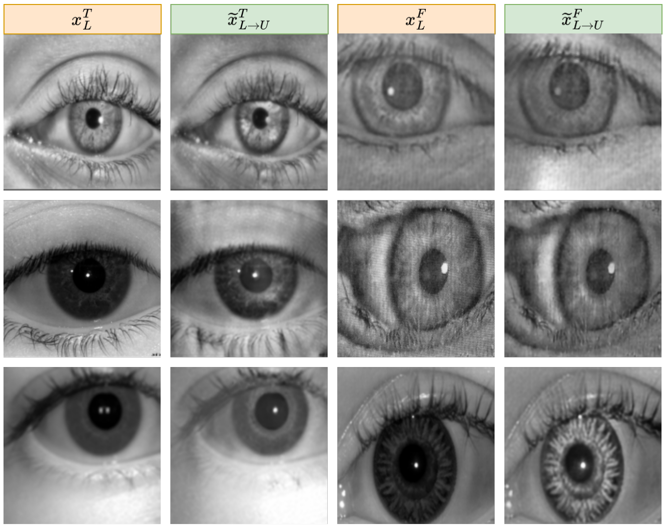

Figure 2: Mapped data examples of different labels.

III. Proposed Approach

We put forth an innovative method known as Refined System-Unsupervised Domain Adaptation (RS-UDA), devised to harness pertinent information from disparate domains and fortify the classifier's training process. A comprehensive diagram of the RS-UDA framework is given in Figure 1. Our strategy incorporates the development of a resilient iris Presentation Attack Detection (PAD) model utilizing two types of data: unprocessed labeled data represented as x_L, and labeled data transitioned from the source domain to the target domain, designated as $\tilde{x}_{L\to U}$, using the Contrastive Unpaired Translation (CUT) technique [56]. We employ two CUT networks, one targeting the bona fide iris samples (y_T) labeled as positive-CUT, and the other managing attack presentations (y_F) under the negative-CUT banner. The correspondence between the source and target domains hinges on the classifier's prognostications.

With each epoch, the classifier's inference gives rise to pseudo-labels. Data instances that surpass a predetermined confidence level set by the model (0.85 in our research) are amassed to denote the data distribution for each label. Consequently, the CUT networks are trained to ascertain the transformation from the source to the target domains. It's worth noting that the data input to the CUT networks is dynamically chosen based on the predictions at each epoch. Representative transformations between the domains are exhibited in Figure 2.

A. Contrastive Unpaired Translation

Contrastive Unpaired Translation (CUT) [56] is a novel method for unpaired image-to-image translation that maximizes mutual information between input and output patches using a framework based on noise contrastive estimation [57]. CUT is a relatively simple and efficient method that achieves superior performance compared to existing methods, while reducing training time and memory usage.

The CUT method is based on the idea of maximizing mutual information between input and output patches, which is achieved by minimizing the contrastive loss between positive and negative pairs of patches. Positive pairs are patches from the same image, while negative pairs are patches from different images. By minimizing the contrastive loss, CUT encourages the generator to produce output patches $\boldsymbol{v}$ that are similar to the corresponding input patches $\boldsymbol{v}^+$, while being dissimilar to other input patches $\boldsymbol{v}^-$. The contrastive loss between positive and negative pairs of patches can be expressed as follows:

$$l(\boldsymbol{v}, \boldsymbol{v}^+, \boldsymbol{v}^-) = \frac{\exp\left(\boldsymbol{v}\cdot\boldsymbol{v}^+/\tau\right)}{\exp\left(\boldsymbol{v}\cdot\boldsymbol{v}^+/\tau\right) + \sum_{n=1}^{N}\exp\left(\boldsymbol{v}\cdot\boldsymbol{v}^-/\tau\right)} \qquad (1)$$

CUT is a one-sided translation method, which means that it only requires a single generator to translate images from one domain to another, without the need for a second generator or a cycle-consistency loss. This makes CUT more memory-efficient and faster than other methods, while still achieving superior performance on image quality metrics such as mAP, pixel-wise accuracy, and average class accuracy.

CUT can be used in a variety of applications, including style transfer, image colorization, and semantic segmentation. It is a practical and efficient alternative to other image-to-image translation methods, especially in scenarios where an image translation model is jointly trained with other components. Overall, CUT is a promising method for unpaired image-to-image translation that offers a simple and efficient solution to a challenging problem.

B. Warm-up Procedure

The functionality of our proposed RS-UDA method is significantly influenced by the caliber of pseudo-labels. Consequently, a preliminary warm-up stage is incorporated into the overarching algorithm. During the initial α epochs, training is confined solely to the classifier and utilizes labeled data. For the subsequent β epochs, the two CUT networks undertake training for the transformation from the source domain to the target domain. Post this collective $\alpha + \beta$ warm-up epochs, the mapped data commences participation in the classifier's training process.

C. Classifier Backbone

The advanced RS-UDA method we propose allows the use of any image-classification-based model as a classifier. In our research, we have opted for EfficientNet [58] as our preferred classifier. Renowned in recent years, EfficientNet is a convolutional neural network architecture designed for generic image classification tasks and has earned significant acclaim. It is notable for its capability to establish an optimal balance between the number of parameters and the total performance. This attribute renders it a suitable selection for our research pursuits, where our aim is to secure the best possible classification outcomes while reducing computational complexity to a minimum.

Table I: COMPOSITION OF THE DATASETS.

	Train			Test known			Test unknown		
Iris Database	Live	Contacts	Printouts	Live	Contacts	Printouts	Live	Contacts	Printouts
Clarkson	2,469	1,122	1,346	1,485	765	908	638	494	144
IIITD-WYU	2,250	1,000	3,000	-	-	-	702	701	2,806
Notre Dame	600	600	-	900	900	-	900	900	-
Warsaw	1,844	-	2,669	974	-	2,016	2,350	-	2,160

IV. EXPERIMENTS

A. Datasets

Our proposed methodology's assessment was carried out utilizing the LivDet-Iris 2017 dataset [10], initially comprised of four subsets. Due to the inaccessibility of the Warsaw dataset, we confined our evaluation to the remaining subsets: Clarkson, Notre Dame, and IIITD-WVU.

The Clarkson subset encompasses a diversity of images, encompassing live irises, textured contact lenses, and iris printouts. Conversely, the Warsaw subset houses images of live irises and iris printouts. The Notre Dame subset presents us with images of live irises both with and without textured contact lenses. Lastly, the IIITD-WVU subset incorporates images of live irises, textured contact lenses, iris printouts, in addition to textured contact lens printouts. For a detailed summary of the configuration of the dataset, see Table I.

Each dataset in the LivDet-Iris 2017 competition is bifurcated into two segments: a train partition supplied to participants for algorithmic training, and a test partition retained by the organizers for the appraisal of submissions. The LivDet-Iris 2017 co-organizers classified their test samples into two clusters. The first cluster, termed as "test known," includes images where live samples and artifacts share identical properties to the train samples. The second cluster, referred to as "test unknown," houses images that exhibit dissimilar or "unknown" properties compared to those in the train subsets.

Different strategies were deployed by the competition organizers to generate the test unknown samples. Clarkson University incorporated visible-light image printouts and introduced new textured contact lens patterns. Warsaw University of Technology employed varied equipment to fabricate and photograph iris printouts. The University of Notre Dame provided images of patterned contact lenses from brands distinct from those present in the train set. The entire test partition of the IIITD-WVU benchmark is treated as test unknown due to its collection by a distinct institution (WVU) using a unique sensor, and it includes outdoor acquisitions. Sample images from each dataset are exhibited in Figure 3.

In adherence to the LivDet-Iris 2017 evaluation protocol, our methods are trained exclusively using the predefined training partitions of the datasets. Subsequently, the final performance of our methods is estimated by evaluating them on both the test known and test unknown partitions. This ensures compliance with the evaluation standards set forth by LivDet-Iris 2017.

B. Experimental Protocol

The experiments conducted in our study strictly followed the evaluation protocol of the LivDet-Iris 2017 competition [10]. We utilized the same datasets and train/test partitions as described in Section IV-A. During the training process, our system was trained to perform binary classification. Authentic iris images were labeled as "live," while attack images, including textured contact lenses, printouts of live images, or printouts of textured contact lenses, were labeled as "attack."

The performance of our classifiers is assessed using four key metrics:

- *Accuracy*: This metric calculates the ratio between the number of correctly classified images and the total number of classified images.
- *Bona-Fide Presentation Classification Error Rate (BPCER)*: BPCER measures the proportion of live images that are incorrectly classified as attacks.
- *Attack Presentation Classification Error Rate (APCER)*: APCER quantifies the proportion of attack images that are incorrectly classified as live samples.
- *Half Total Error Rate (HTER)*: HTER is the average of BPCER and APCER, providing an overall measure of performance.

The BPCER and APCER error rates are defined by ISO/IEC 30107-3 [59] and were adopted in the LivDet-Iris 2017 competition for evaluating submissions. During the training stage, accuracy and HTER are used to rank the obtained solutions. The CNN classifiers employed in our study generate liveness scores ranging from 0 to 1, with a decision threshold of 0.5, as specified in the LivDet-Iris 2017 protocol.

C. Intra-Database Testing

We commence with intra-database testing on each dataset individually. As illustrated by the tabulated results in Table II, it becomes evident that the proposed methods exhibit a superior representation capacity compared to the existing methodologies. Furthermore, we observe that the proposed RS-UDA secures a significantly lower HTER. These findings indicate the greater effectiveness of our approach in acquiring a discriminative feature representation for the classification of live versus spoof iris images. Additionally, it's noticeable that the FAM [16] also exhibits effectiveness in the PAD task.

D. Cross-Domain Evaluation

Our method is compared with existing state-of-the-art methods in Table III. The data reveals that our

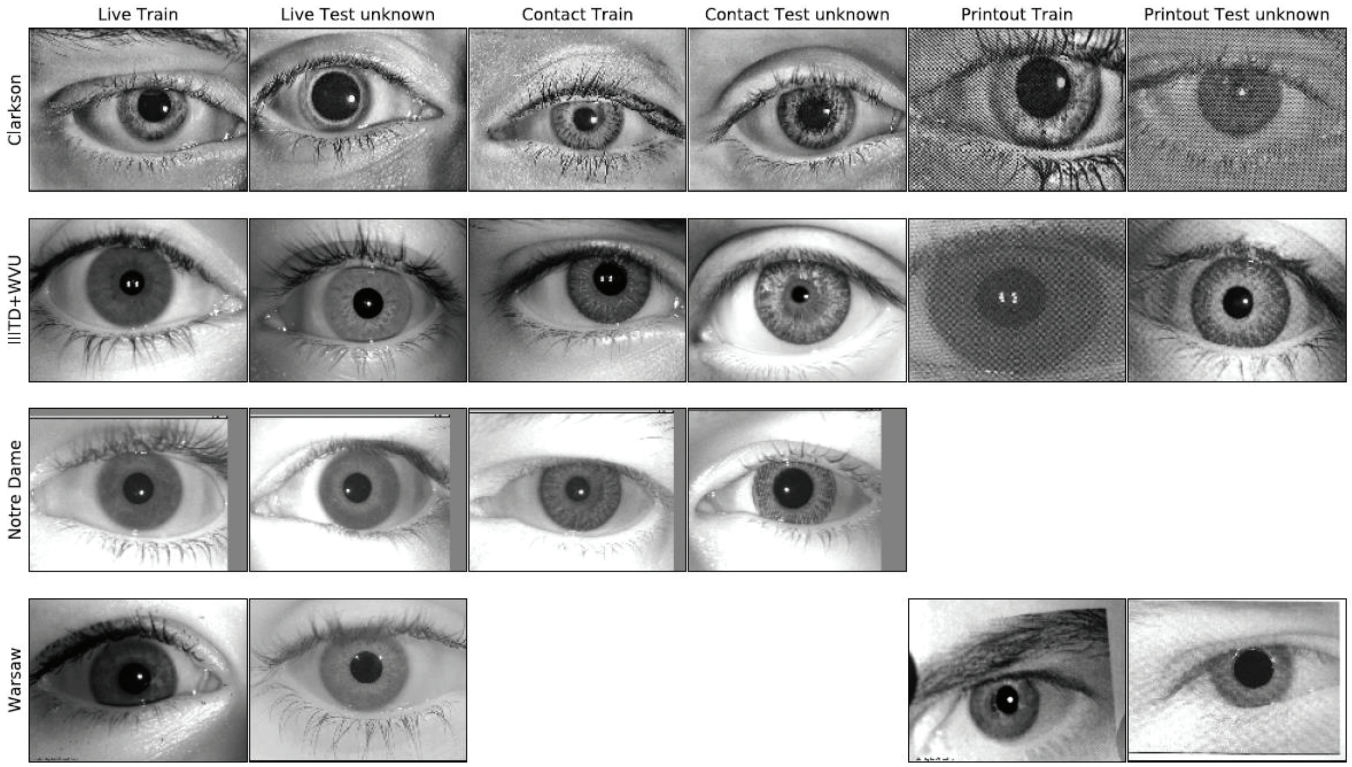

Figure 3: Image samples extracted from the LivDet-Iris 2017 dataset (image from [14]), showcasing both the train and unknown partitions.

Table II: Comparison to existing SoTA methods on LivDet-Iris 2017 dataset under intra-dataset settings.

		PAD Algorithm							
Database	Metric	CASIA[10]	SpoofNet[39]	D-NetPAD[12]	MSA[60]	PBS[15]	A-PBS[15]	FAM[16]	our
Clarkson	APCER	13.39	33.00	5.78	-	8.97	6.16	6.10	2.33
	BPCER	0.81	0.00	0.94	-	0.00	0.81	0.81	0.47
	HTER	7.10	16.50	3.36	-	4.48	3.48	3.45	1.40
NotreDame	APCER	7.78	18.05	10.38	12.28	8.89	7.88	8.06	3.06
	BPCER	0.28	0.94	3.32	0.17	1.06	0.00	0.00	0.39
	HTER	4.03	9.50	6.84	6.23	4.97	3.94	4.03	1.72
IIIT-WVU	APCER	29.40	0.34	36.41	2.31	5.76	8.86	1.00	5.70
	BPCER	3.99	36.89	10.12	19.94	8.26	4.13	12.68	7.41
	HTER	16.70	18.62	23.27	11.13	7.01	6.50	6.84	6.56

method consistently surpasses PBS [15], A-PBS [15], and FAM+FMM [16]. The distinctive style of the Clarkson dataset is noteworthy, especially when we observe a 3.31% and 15.48% improvement when testing on the Notre Dame and IIITD-WVU subsets, respectively. In stark contrast, results achieved through other methodologies all exceed 20%. Our approach integrates source bonafide/attack linked components with style contents from the target domain, thereby substantially elevating performance with negligible costs. It's also significant to note that there's no requirement to modify the model or training pipeline when implementing either intra-dataset or inter-dataset settings.

E. Ablation Study

We provide ablation study to investigate the effectiveness of the three components in our system, i.e., (i) , (ii) , and (iii) . We study their influences by gradually dropping them from , and denote the corresponding models as w/o , w/o , w/o , w/o & , w/o &, w/o & and w/o & & .

The results of these models under cross-database testing on CASIA, Idiap, MSU and Rose-Youtu are given in Table X and Fig. X. We can see dropping any of the three components will lead to increased PAD error. This suggests that all the three components are useful for our XXX approach. In addition, we notice that X has a bigger influence than the other two modules to the generalization abilities of the proposed method. For example, respectively. The possible reason is that . For example, if we visualize the feature representation learned by alone, w/o and the whole , we can see using and together with can obtain more robust feature representations that are discriminative for genuine vs. spoof face image classification . We also conduct statistical t-test for the proposed approach under ablation study. In addition, compared with the results by discarding all three components, the full method shows signification improvement in cross-dataset testing.

Table III: Comparison to existing SoTA methods on LivDet-Iris 2017 dataset under cross-dataset settings.

Trained Dataset	IIITD-WVU		NotreDame		Clarkson	
Tested Dataset	NotreDame	Clarkson	IIITD-WVU	Clarkson	IIITD-WVU	NotreDame
PBS	16.86	47.17	17.49	45.31	42.48	32.42
A-PBS	27.61	21.99	9.49	22.46	34.17	23.08
FAM+FMM	5.81	26.03	15.07	10.51	22.06	20.92
(Ours)	4.50	12.20	11.78	8.93	15.48	3.31

V. Conclusions

This paper addresses cross-domain iris presentation attack detection (PAD)and proposes an unsupervised adversarial domain adaptation method that can leverage unlabeled target domain data and labeled source domain data to build robust PAD model. the proposed system consists of Positive-CUTGAN Net(PC-Net), Negtive-CUTGAN Net(NC-Net) and Iterative(I-Net). NC-Net and IR-Net transfer the raw imaged of target domain into the synthetic images of source domain. I-Net drive the above Nets iteratively and obtain the dataset precise progressively. The proposed approach outperforms the state-of-the-art iris PAD methods on the a number of the public databases under the challenging cross-database testing scenario. Our future work includes utilizing starGAN and self-traning cues to further improve the robustness of PAD models. In addition, we will study how to learn better representations that can further reduce the domain gap during domain adaptation.

References

[1] J. G. Daugman and C. Downing, "Epigenetic randomness, complexity and singularity of human iris patterns," *Proceedings of the Royal Society of London. Series B: Biological Sciences*, vol. 268, pp. 1737 – 1740, 2001.

[2] K. Bowyer and P. J. Flynn, "Biometric identification of identical twins: A survey," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–8, 2016.

[3] J. E. Tapia, C. A. Pérez, and K. Bowyer, "Gender classification from the same iris code used for recognition," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1760–1770, 2016.

[4] J. McGrath, K. Bowyer, and A. Czajka, "Open source presentation attack detection baseline for iris recognition," *ArXiv*, vol. abs/1809.10172, 2018.

[5] G. of India, "Unique identification authority of india website."

[6] J. G. Daugman, "600 million citizens of india are now enrolled with biometric id," *Spie Newsroom*, 2014.

[7] "Canada border services agency and u.s. customs and border protection."

[8] S. I. 30107-1, "Information technologybiometric presentation attack detectionpart 1: Framework," 2016.

[9] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.

[10] D. Yambay, B. Becker, N. Kohli, D. Yadav, A. Czajka, K. Bowyer, S. Schuckers, R. Singh, M. Vatsa, A. Noore, D. Gragnaniello, C. Sansone, L. Verdoliva, L. He, Y. Ru, H. Li, N. Liu, Z. Sun, and T. Tan, "Livdet iris 2017 iris liveness detection competition 2017," *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 733–741, 2017.

[11] D. Yadav, N. Kohli, J. S. Doyle, R. Singh, M. Vatsa, and K. Bowyer, "Unraveling the effect of textured contact lenses on iris recognition," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 851–862, 2014.

[12] R. Sharma and A. A. Ross, "D-netpad: An explainable and interpretable iris presentation attack detector," *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–10, 2020.

[13] A. Boyd, Z. Fang, A. Czajka, and K. Bowyer, "Iris presentation attack detection: Where are we now?," *Pattern Recognit. Lett.*, vol. 138, pp. 483–489, 2020.

[14] A. Kuehlkamp, A. da Silva Pinto, A. Rocha, K. Bowyer, and A. Czajka, "Ensemble of multi-view learning classifiers for cross-domain iris presentation attack detection," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 1419–1431, 2018.

[15] M. Fang, N. Damer, F. Boutros, F. Kirchbuchner, and A. Kuijper, "Iris presentation attack detection by attention-based and deep pixel-wise binary supervision network," *2021 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–8, 2021.

[16] Y. Li, Y. Lian, J. Wang, Y. Chen, C. Wang, and S. Pu, "Few-shot one-class domain adaptation based on frequency for iris presentation attack detection," *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2480–2484, 2022.

[17] H. Li, W. Li, H. Cao, S. Wang, F. Huang, and A. C. Kot, "Unsupervised domain adaptation for face anti-spoofing," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 1794–1809, 2018.

[18] H. Li, P. He, S. Wang, A. Rocha, X. Jiang, and A. C. Kot, "Learning generalized deep feature representation for face anti-spoofing," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 2639–2652, 2018.

[19] J. G. Daugman, "Wavelet demodulation codes, statistical independence, and pattern recognition," 2000.

[20] L. Thalheim, J. Krissler, and P.-M. Ziegler, "Body check: Biometric access protection devices and their programs put to the test," 04 2023.

[21] A. N. Al-Raisi and A. M. Al-Khouri, "Iris recognition and the challenge of homeland and border control security in uae," *Telematics Informatics*, vol. 25, pp. 117–132, 2008.

[22] J. S. Doyle, P. J. Flynn, and K. Bowyer, "Automated classification of contact lens type in iris images," *2013 International Conference on Biometrics (ICB)*, pp. 1–6, 2013.

[23] X. He, Y. Lu, and P. Shi, "A new fake iris detection method," in *International Conference on Biometrics*, 2009.

[24] J. Zuo, N. A. Schmid, and X. Chen, "On generation and analysis of synthetic iris images," *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 77–90, 2007.

[25] M. Trokielewicz, A. Czajka, and P. Maciejewicz, "Human iris recognition in post-mortem subjects: Study and database," *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–6, 2016.

[26] J. Komulainen, A. Hadid, and M. Pietikäinen, "Generalized textured contact lens detection by extracting bsif description from cartesian iris images," *IEEE International Joint Conference on Biometrics*, pp. 1–7, 2014.

[27] Lovish, A. Nigam, B. Kumar, and P. Gupta, "Robust contact lens detection using local phase quantization and binary gabor pattern," in *International Conference on Computer Analysis of Images and Patterns*, 2015.

[28] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "An investigation of local descriptors for biometric spoofing detection," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 849–863, 2015.

[29] A. F. Sequeira, S. Thavalengal, J. M. Ferryman, P. M. Corcoran, and J. S. Cardoso, "A realistic evaluation of iris presentation attack detection," *2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 660–664, 2016.

[30] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Contact lens detection and classification in iris images through scale invariant descriptor," *2014 Tenth International Conference on*

Signal-Image Technology and Internet-Based Systems, pp. 560–565, 2014.

[31] F. Pala and B. Bhanu, "Iris liveness detection by relative distance comparisons," *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 664–671, 2017.

[32] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "Mobio_livdet: Mobile biometric liveness detection," *2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pp. 187–192, 2014.

[33] R. Chen, X. Lin, and T. Ding, "Liveness detection for iris recognition using multispectral images," *Pattern Recognit. Lett.*, vol. 33, pp. 1513–1519, 2012.

[34] J. Galbally, M. Savvides, S. Venugopalan, and A. A. Ross, "Iris image reconstruction from binary templates," 2016.

[35] P. H. L. Silva, E. J. da S. Luz, R. Baeta, H. Pedrini, A. X. Falcão, and D. Menotti, "An approach to iris contact lens detection based on deep image representations," *2015 28th SIBGRAPI Conference on Graphics, Patterns and Images*, pp. 157–164, 2015.

[36] R. Raghavendra, K. B. Raja, and C. Busch, "Contlensnet: Robust iris contact lens detection using deep convolutional neural networks," *2017 IEEE Winter Conference on Applications of Computer Vision (WACV)*, pp. 1160–1167, 2017.

[37] H. Zou, H. Zhang, X. Li, J. Liu, and Z. He, "Generation textured contact lenses iris images based on 4dcycle-gan," *2018 24th International Conference on Pattern Recognition (ICPR)*, pp. 3561–3566, 2018.

[38] D. Gragnaniello, C. Sansone, G. Poggi, and L. Verdoliva, "Biometric spoofing detection by a domain-aware convolutional neural network," *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp. 193–198, 2016.

[39] G. Y. Kimura, D. R. Lucio, A. de Souza Britto, and D. Menotti, "Cnn hyperparameter tuning applied to iris liveness detection," *ArXiv*, vol. abs/2003.00833, 2020.

[40] A. Boyd, A. Czajka, and K. Bowyer, "Deep learning-based feature extraction in iris recognition: Use existing models, fine-tune or train from scratch?," *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–9, 2019.

[41] T. D. Nguyen, N. R. Baek, T. D. Pham, and K. R. Park, "Presentation attack detection for iris recognition system using nir camera sensor," *Sensors (Basel, Switzerland)*, vol. 18, 2018.

[42] Y. Ganin and V. S. Lempitsky, "Unsupervised domain adaptation by backpropagation," *ArXiv*, vol. abs/1409.7495, 2014.

[43] G. Csurka, "Domain adaptation for visual applications: A comprehensive survey," *ArXiv*, vol. abs/1702.05374, 2017.

[44] M. Long, Y. Cao, J. Wang, and M. I. Jordan, "Learning transferable features with deep adaptation networks," *ArXiv*, vol. abs/1502.02791, 2015.

[45] M. Long, H. Zhu, J. Wang, and M. I. Jordan, "Unsupervised domain adaptation with residual transfer networks," in *NIPS*, 2016.

[46] M. Ghifary, W. Kleijn, M. Zhang, D. Balduzzi, and W. Li, "Deep reconstruction-classification networks for unsupervised domain adaptation," *ArXiv*, vol. abs/1607.03516, 2016.

[47] M. Mirza and S. Osindero, "Conditional generative adversarial nets," *ArXiv*, vol. abs/1411.1784, 2014.

[48] E. Tzeng, J. Hoffman, K. Saenko, and T. Darrell, "Adversarial discriminative domain adaptation," *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 2962–2971, 2017.

[49] M.-Y. Liu, T. M. Breuel, and J. Kautz, "Unsupervised image-to-image translation networks," in *NIPS*, 2017.

[50] H. Li, W. Li, H. Cao, S. Wang, F. Huang, and A. C. Kot, "Unsupervised domain adaptation for face anti-spoofing," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 1794–1809, 2018.

[51] G. Wang, H. Han, S. Shan, and X. Chen, "Unsupervised adversarial domain adaptation for cross-domain face presentation attack detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 56–69, 2021.

[52] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823, 2015.

[53] I. Misra and L. van der Maaten, "Self-supervised learning of pretext-invariant representations," *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 6706–6716, 2019.

[54] T. Chen, S. Kornblith, M. Norouzi, and G. E. Hinton, "A simple framework for contrastive learning of visual representations," *ArXiv*, vol. abs/2002.05709, 2020.

[55] P. Khosla, P. Teterwak, C. Wang, A. Sarna, Y. Tian, P. Isola, A. Maschinot, C. Liu, and D. Krishnan, "Supervised contrastive learning," *ArXiv*, vol. abs/2004.11362, 2020.

[56] T. Park, A. A. Efros, R. Zhang, and J.-Y. Zhu, "Contrastive learning for unpaired image-to-image translation," in *European Conference on Computer Vision*, 2020.

[57] A. van den Oord, Y. Li, and O. Vinyals, "Representation learning with contrastive predictive coding," 2019.

[58] M. Tan and Q. V. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," 2020.

[59] S. I. 30107-3, "Information technologybiometric presentation attack detection part 3: Testing and reporting," 2017.

[60] M. Fang, N. Damer, F. Kirchbuchner, and A. Kuijper, "Micro stripes analyses for iris presentation attack detection," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–10, 2020.