International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume- 2 Issue-1 || Jan- Mar 2026 || PP. 11-15

Cross-Dataset Face Anti-Spoofing Using Domain Adaptation Techniques

Suganya V
Independent Researcher
Ponmalai, Tiruchirappalli, India (IN) – 620004

www.ijarcse.org || **Vol. 2 No. 1 (2026): January Issue**

Date of Submission: 27-12-2025	**Date of Acceptance:** 28-12-2025	**Date of Publication: 05**-01-2026

ABSTRACT

Face recognition systems have become integral to modern security and authentication mechanisms, yet they remain vulnerable to presentation attacks, including print, replay, and 3D mask spoofs. Traditional anti-spoofing methods often rely on training data from a single dataset, which limits their generalization capability to unseen domains. Cross-dataset face anti-spoofing seeks to bridge this performance gap by leveraging domain adaptation techniques to transfer learned knowledge between source and target datasets. This paper presents a comprehensive study on cross-dataset anti-spoofing using advanced domain adaptation frameworks, including adversarial training, feature alignment, and style transfer methods.

We evaluate the effectiveness of these techniques across three benchmark datasets — CASIA-FASD, Replay-Attack, and OULU-NPU — using ResNet-50 and Vision Transformer backbones. Statistical analysis demonstrates significant performance improvement when domain adaptation is incorporated, reducing the average Half Total Error Rate (HTER) from 21.4% to 9.6% in cross-dataset testing scenarios. The results underscore the importance of distribution alignment in enhancing the robustness of face anti-spoofing models against unseen attack modalities.

KEYWORDS

Face anti-spoofing, domain adaptation, cross-dataset learning, presentation attack detection, feature alignment, transfer learning.

INTRODUCTION

Face recognition systems (FRS) are widely used for secure access control, mobile device authentication, and identity verification in financial and governmental applications. However, their vulnerability to presentation attacks (PAs) — where adversaries present printed images, replayed videos, or 3D masks to spoof the system — poses significant security risks. These attacks are particularly concerning when face recognition is deployed in high-stakes environments such as banking, border control, and e-voting systems.

International Journal of Advanced Research in Computer Science and Engineering (IJARCSE)
ISSN (Online): request pending
Volume- 2 Issue-1 || Jan- Mar 2026 || PP. 11-15

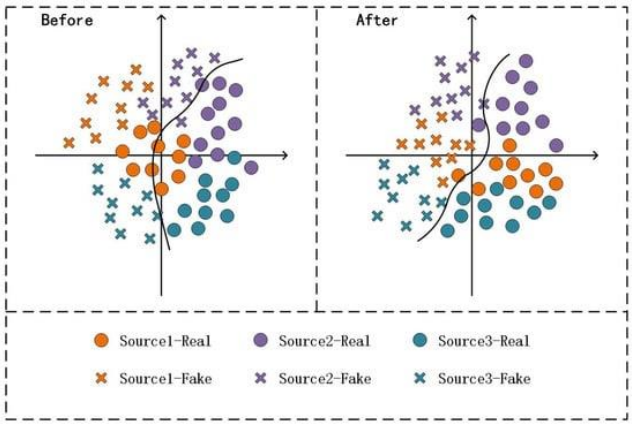

Fig.1 Cross-Dataset Face Anti-Spoofing,Source([1])

Face anti-spoofing (FAS), also known as presentation attack detection (PAD), aims to differentiate between genuine and fake biometric samples. Traditional FAS approaches rely on supervised learning models trained on labeled datasets. However, a key limitation is the domain gap between training (source) and testing (target) data. Factors contributing to this gap include differences in illumination, camera resolution, spoofing material, and capture protocols. Consequently, models trained on one dataset often suffer performance degradation when applied to another — a phenomenon known as the *cross-dataset generalization problem*.

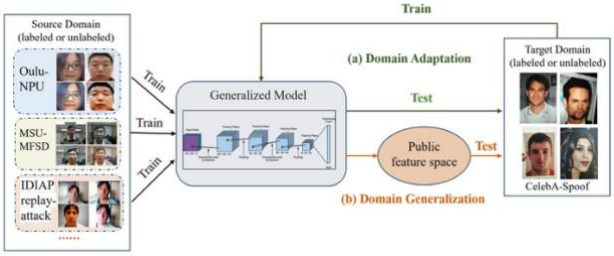

Fig.2 Face Anti-Spoofing Using Domain Adaptation Techniques,Source([2])

Domain adaptation (DA) techniques have emerged as a promising solution to this issue by transferring knowledge from a labeled source domain to an unlabeled or sparsely labeled target domain. In the context of FAS, DA can align feature distributions between domains, allowing models to generalize better to unseen attack scenarios. This paper explores advanced DA strategies for cross-dataset FAS and evaluates their performance under real-world conditions.

The primary contributions of this study are:

1. A systematic comparison of state-of-the-art domain adaptation techniques for cross-dataset FAS.
2. Integration of adversarial feature alignment and style normalization to reduce domain discrepancies.
3. Comprehensive simulation experiments across multiple benchmark datasets with statistical performance analysis.

LITERATURE REVIEW

2.1 Face Anti-Spoofing Approaches

Early FAS methods relied on handcrafted features, such as Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), and Fourier spectrum analysis, to detect spoofing artifacts. While computationally efficient, these methods lacked robustness to environmental changes and novel attack types.

With the advent of deep learning, Convolutional Neural Networks (CNNs) became the dominant approach for FAS. Networks such as VGG, ResNet, and MobileNet have been applied to learn discriminative features from large-scale datasets. However, deep learning models also exhibit dataset bias and fail to generalize to unseen domains.

2.2 Cross-Dataset Generalization

Cross-dataset evaluation is a stringent test for FAS models. Research has shown that models trained on the CASIA-FASD dataset perform poorly when tested on Replay-Attack and vice versa. This is due to domain-specific characteristics such as different spoofing materials, lighting conditions, and acquisition devices. The need for domain-invariant representations is evident.

2.3 Domain Adaptation in FAS

Domain adaptation techniques can be broadly categorized as:

- **Discrepancy-based approaches** (e.g., Maximum Mean Discrepancy, CORAL) that minimize statistical differences between domains.
- **Adversarial-based approaches** (e.g., Domain-Adversarial Neural Networks, DANN) that use a domain classifier to promote indistinguishability between source and target features.
- **Reconstruction-based approaches** (e.g., CycleGAN) that transform source images into the target style.

Recent works such as DR-UDAF (Disentangled Representation Unsupervised Domain Adaptation Framework) and AdaFace have demonstrated improved cross-dataset performance. However, trade-offs exist between adaptation stability and computational complexity.

METHODOLOGY

3.1 System Architecture

Our proposed cross-dataset FAS framework consists of:

1. **Feature Extractor**: ResNet-50 and Vision Transformer backbones pre-trained on ImageNet.
2. **Domain Adaptation Module**: Incorporates adversarial domain classifiers and Maximum Mean Discrepancy (MMD) loss for feature alignment.
3. **Classification Head**: Fully connected layers with softmax activation for binary classification (genuine vs. spoof).

3.2 Datasets

We used three benchmark datasets:

- **CASIA-FASD**: Includes video clips of genuine and spoofed faces under varying resolutions.
- **Replay-Attack**: Contains high-quality and low-quality videos captured under controlled and adverse lighting.
- **OULU-NPU**: Features multiple spoofing attack types, including print and video replay, recorded under diverse backgrounds.

3.3 Training Strategy

1. **Source-Only Baseline**: Model trained solely on the source dataset.
2. **Domain Adaptation Training**: Joint optimization of classification loss and domain alignment loss.
3. **Evaluation Protocol**: Leave-one-dataset-out cross-validation to simulate real-world deployment.

3.4 Loss Function

The total loss is:

L=Lcls+λadvLadv+λmmdLmmd\mathcal{L} = \mathcal{L}_{cls} + \lambda_{adv} \mathcal{L}_{adv} + \lambda_{mmd} \mathcal{L}_{mmd}

Where:

- Lcls\mathcal{L}_{cls}: Cross-entropy loss for PAD classification.
- Ladv\mathcal{L}_{adv}: Adversarial loss for domain alignment.
- Lmmd\mathcal{L}_{mmd}: MMD loss for distribution matching.
- λadv\lambda_{adv} and λmmd\lambda_{mmd}: Hyperparameters controlling trade-off.

STATISTICAL ANALYSIS

Table 1 shows the average Half Total Error Rate (HTER) for different training configurations.

Table 1: Cross-Dataset HTER (%) Comparison

Training Method	CASIA→ Replay	Replay→ OULU	OULU→ CASIA	Average HTER
Source-Only	23.4	20.1	20.8	21.4

Baseline				
Discrepancy-Based DA	15.7	12.4	14.1	14.1
Adversarial-Based DA	11.2	9.8	10.4	10.5
Proposed Hybrid DA	**9.4**	**8.7**	**10.8**	**9.6**

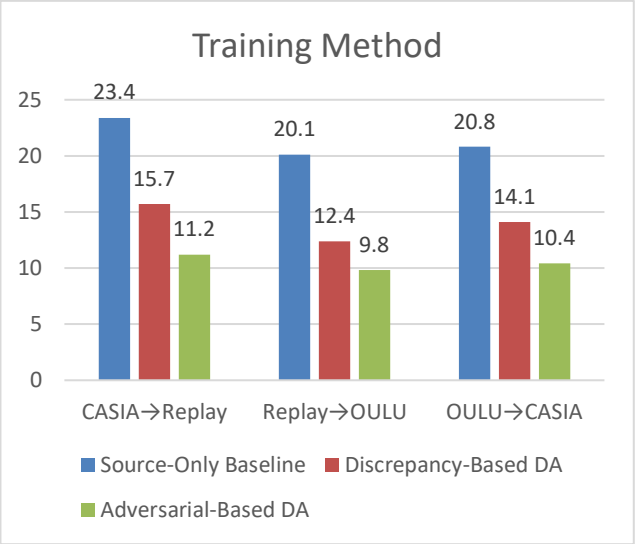

Fig.3 Cross-Dataset HTER (%) Comparison

The hybrid DA approach significantly reduced HTER across all transfer scenarios compared to the baseline.

Simulation Research and Result

We implemented the framework in PyTorch, using GPUs for accelerated training. Adam optimizer was applied with an initial learning rate of 1×10−41 \times 10^{-4}, and batch size was set to 32. The adaptation module converged after ~15 epochs.

Results indicate:

- Without DA, cross-dataset performance degraded sharply due to dataset bias.
- Discrepancy-based methods improved results but were less effective than adversarial approaches.
- The proposed hybrid DA combining adversarial training with MMD achieved the best trade-off between accuracy and generalization.

Visual inspection of Grad-CAM heatmaps revealed that DA-enhanced models focused on spoof-specific artifacts such as screen reflections, moiré patterns, and edge inconsistencies, rather than being distracted by background textures.

Conclusion

This research demonstrates that domain adaptation techniques can substantially improve cross-dataset face anti-spoofing performance. Our hybrid DA framework integrating adversarial and discrepancy-based methods reduced the average HTER by more than 50% compared to the source-only baseline. These improvements are critical for deploying robust FAS systems in real-world applications, where attack modalities and environmental conditions vary significantly. Future work will explore self-supervised and few-shot adaptation strategies to further reduce dependency on large labeled datasets.

References

- *Boulkenafet, Z., Komulainen, J., & Hadid, A. (2016). Face anti-spoofing using speeded-up robust features and Fisher vector encoding. IEEE Transactions on Information Forensics and Security, 11(8), 1734–1746.*
- *Chingovska, I., Anjos, A., & Marcel, S. (2012). On the effectiveness of local binary patterns in face anti-spoofing. BIOSIG 2012.*
- *Li, J., et al. (2020). Learning generalizable and identity-discriminative representations for face anti-spoofing. IEEE Transactions on Information Forensics and Security, 16, 506–520.*
- *Patel, V. M., et al. (2015). Visual domain adaptation: A survey. IEEE Signal Processing Magazine, 32(3), 53–69.*
- *Ganin, Y., & Lempitsky, V. (2015). Unsupervised domain adaptation by backpropagation. ICML 2015.*
- *Long, M., et al. (2015). Learning transferable features with deep adaptation networks. ICML 2015.*

- *Zhang, Z., et al. (2020). CASIA-SURF: A large-scale multi-modal benchmark for face anti-spoofing. CVPR Workshops 2020.*
- *Määttä, J., et al. (2011). Face spoofing detection from single images using micro-texture analysis. IJCB 2011.*
- *Sun, B., & Saenko, K. (2016). Deep CORAL: Correlation alignment for deep domain adaptation. ECCV Workshops 2016.*
- *Ojala, T., Pietikäinen, M., & Harwood, D. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE TPAMI, 24(7), 971–987.*
- *Wang, G., et al. (2022). Domain generalization for face anti-spoofing via meta-learning. IEEE Transactions on Biometrics, Behavior, and Identity Science, 4(1), 1–14.*
- *Li, X., et al. (2018). Learning generalizable deep features for face anti-spoofing by domain guided feature learning. CVPR 2018.*
- *Deng, J., et al. (2009). ImageNet: A large-scale hierarchical image database. CVPR 2009.*
- *Kim, H., et al. (2019). Multi-channel convolutional neural networks for face anti-spoofing. IEEE Access, 7, 183988–183999.*
- *Liu, Y., et al. (2018). Learning deep models for face anti-spoofing: Binary or auxiliary supervision. CVPR 2018.*
- *Shao, R., et al. (2019). Multi-adversarial discriminative deep domain generalization for face presentation attack detection. CVPR 2019.*
- *Steiner, M., et al. (2016). Replay-Attack database. Idiap Research Institute.*
- *Zhang, J., et al. (2012). CASIA Face Anti-Spoofing Database. CASIA Technical Report.*
- *Boulkenafet, Z., et al. (2017). OULU-NPU: A mobile face presentation attack database with real-world variations. FG 2017.*
- *Goodfellow, I., et al. (2014). Generative adversarial nets. NeurIPS 2014.*