[1]Atul Kumar Uttam
[2] Rohit Agarwal
[3]Anand Singh Jalal

Fingerprint Presentation Attack Detection using Unsupervised Divergence Based Domain Adaptation

Journal of Electrical Systems

Abstract: - The biometric system that uses fingerprints is prone to different types of attacks. The presentation attack is one of the easiest to perform on the fingerprint sensor. In recent years, several Fingerprint Presentation Attack Detection (FPAD) approaches have been proposed. These FPAD approaches have attained fair results on a dataset of different materials (cross-material). However, FPAD method performance degrades up to 30% when training and testing datasets are from different distributions (sensors). So for a robust FPAD method, it must learn domain-independent features to have consistent performance. To mitigate the domain-shift and FPAD, we have proposed unsupervised divergence-based domain adaptation (UDDA) with an Adaptive Loss Function (ALF). The ALF integrates domain divergence loss (DDL) and classification loss. The ALF helps in learning domain-invariant features and accurately classifying live and fake fingerprints in a cross-sensor scenario. The investigational outcomes confirmed that the offered UDDA method reduces the cross-sensor average classification error (ACE) by 19.94% and 19.23% on LivDet 2015 and LivDet 2017, respectively.

Keywords: Fingerprint Presentation Attack, Domain Shift, Domain Adaptation, Cross Sensor.

I. INTRODUCTION

The most popular biometric behavior is the fingerprint, which is vulnerable to several kinds of attacks. The presentation attack (PA) [27] is among the simplest attacks to perform on a sensor to interfere with the biometric system's policy [28]. In PA, the attacker without having extensive knowledge of the biometrics system can hamper the operation of the biometrics system with a fake fingerprint made of different materials. Hence it is quite necessary to detect presentation attacks by correctly identifying fake and live fingerprints.

Even though there has been tremendous advancement in the fingerprint presentation attack detection (FPAD) approaches, fails to generalize when the fake fingerprint is made of a novel material not used in training such models. There has been seen up to a three-fold drop in performance in such cross-material generalization scenarios [29]. In recent years, many handcrafted [4-9] and deep feature-based FPAD methods [10-20] have enhanced the generalization performance in cross-material cases. Nevertheless, these FPAD techniques only achieve poor classification accuracy when they are evaluated on fingerprint photos from a different sensor (target dataset) after being trained on images from one sensor (source dataset).

The FPAD approaches suffer from poor sensor interoperability [30], due to domain shifts in source and target datasets. The fingerprint pictures from various sensors have distinct textural appearances, which is the cause of this domain shift (Figure 1). The photographs' properties are solely determined by the illumination, the presenting attack's creator's experience, and the acquisition technique [31]. The domain changes in the source (training) and the target (testing) dataset makes it difficult for the FPAD methods to generalize in a cross-sensor setting.

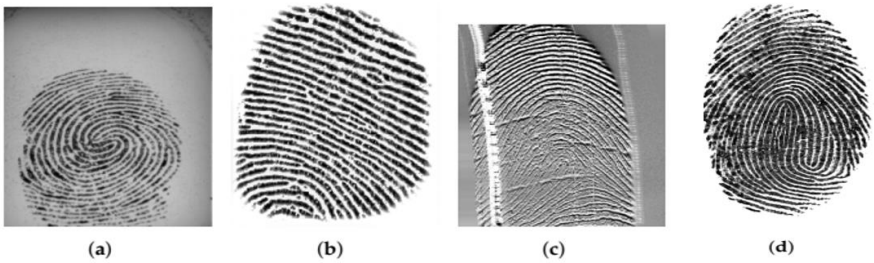

Fig. 1. Examples of LivDet 2015 [22] dataset fingerprints acquired with various sensors: (a) Biometrika, (b) Digital Persona, (c) Orcanthus, (d) GreenBit.

[1] *Corresponding author: atul.uttam @gla.ac.in, Department of Computer Engineering and Applications, GLA University, Mathura, U.P. India
[2] rohit.agrwal@gla.ac.in, Department of Computer Engineering and Applications, GLA University, Mathura, U.P. India
[3] asjalal@gla.ac.in, Department of Computer Engineering and Applications, GLA University, Mathura, U.P. India

To improve the generalization performance when training and test sensors are different, this article proposes a novel FPAD method using unsupervised divergence-based domain adaptation (UDDA). The proposed method utilizes a new adaptive loss function (ALF) which integrates cross entropy loss and Maximum Mean Discrepancy (MMD) [2] or Correlation Alignment (CORAL) [3] loss for domain-independent features learning. The objective is to minimize the distributional difference between the source sensor and target sensor representations to improve the model's generalization to the target sensor in a cross-sensor setting. The following is the proposed work's primary contribution:

- We have designed an unsupervised domain adaptation-based FPAD method (UDDA), which has been used first time for fingerprint presentation attack detection.
- We have also designed a novel adaptive loss function (ALF) to learn domain invariant features and classify fake and live fingerprints accurately.
- The ALF integrates cross-entropy loss and MMD with Gaussian kernel loss or CORAL loss to learn the domain-independent features to enhance the cross-sensor performance.
- The extensive experiment shows that both MMD and CORAL loss enhance PAD performance significantly over the target domain.
- The UDDA utilizes ResNet as the base CNN model for feature extraction which can be integrated with any CNN model easily.

The remainder of the study has been prepared as follows: Section 2 lists important studies related to FPAD. Details of the suggested FPAD model are provided in Section 3. Section 4 provides the conclusion and discussion. Section 5 discusses the conclusion and next steps.

II. Related Work

Several academics have suggested FPAD solutions based on deep learning-based techniques and handmade characteristics to detect presentation assaults over fingerprint biometrics. This section presents some cutting-edge FPAD techniques that target generalization issues brought on by novel materials and/or sensors that weren't employed during FPAD method training.

A. Handcrafted features-based FPAD methods

To quantify and mitigate the effect of novel spoof material Rattani et al. [4] have utilized LBP, LPQ, and BSIF features and applied W-SVM for PA detection tasks. Their study highlights that there is a 97% rise in the rate of errors when a FPAD method is tested on fingerprint images made up of novel spoof material. Their method based on WSVM improves up to 44% in performance in the detection of fingerprints of novel spoof material. Ding et al. [5] have utilized an ensemble method based on One Class SVM (OC-SVM) to improve generalization performance over unseen materials. They first extracted local texture features using LBP, GLCM, BSIF, LPQ, and BGP. Further, these features have been passed to respective OC-SVMs to form an ensemble model. Yuan et al. [6] have suggested a Local Gradient Pattern (LGP) for efficient texture enhancement along with a deep residual network for enhanced generalization performance over unknown spoof material. A Weber local binary descriptor (WLBD) has been proposed by Xia et al. [7] for fingerprint presentation attack detection. For PAD, Sharma et al. [8] have suggested texture descriptors called Uniform LBP (ULBP) and Local Adaptive LBP (LABP). In a different work, Sharma et al. [9] provided an ensemble model for the FPAD problem that combined an eight-layer CNN architecture with a Complete Local Binary Pattern (CLBP) with LALBP.

B. Deep learning-based FPAD methods

Nogueira et al. [10] first applied VGG-CNN and compared the CNN-based model with the LBP-based handcrafted method for FPAD. They first studied the effect of unknown sensor and unknown material cases on the generalization capability of the suggested FPAD method. Marasco et al. [11] have presented a comparison of various CNN models (CaffeNet, GoogleNet, and Siamese) for FPAD. In their study, they have highlighted that the generalization of the FPAD model over novel spoof material can be improved with effective utilization of CNN, but sensor interoperability is still a big concern for degraded performance. Park et al. [12] have suggested a FPAD method that utilizes fingerprint patches. Their method first divides the input fingerprint into no overlapping patches. Further, these patches are passed to the SqueezeNet-CNN for classification of each patch as fake or live and then aggregated the result based on a voting method for final classification. Their method shows better generalization over the novel spoof material. Pala et al. [13] have proposed TripletNet-CNN for FPAD and

generalization over unknown material and sensor scenarios. They have affirmed that generalization to the new sensor is much more difficult than new materials. Chugh et al. [14] have proposed Inception v3-based CNN for FPAD. To enhance the generalization performance over cross-material and cross-sensor cases they have extracted minutiae-centered patches from fingerprints for the PAD task. Zhang et al. [15] have suggested the FPAD method based on an improved residual block to reduce the parameters for a lightweight model. Liu et al. [16] have proposed a MobileNet-based rethinking global-local model for PAD. Agarwal et al. [17] have utilized incremental learning for FPAD tasks. Their model utilizes ResNet-50 for feature extraction and effectively improves the generalization performance over novel materials. Chugh et. al. [18] have utilized a universal material generator and proposed a wrapper-based approach that enhances the generalization performance of FPAD methods. Rai et al. [19] have proposed an ensemble network based on MobileNet and SVM. Their model effectively generalizes cross-material scenarios but is not able to perform similarly in cross-sensor cases. In another study, Rai et al. [20] proposed an ensemble-based model that utilizes deep features and handcrafted features.

Most of the FPAD methods discussed above have a robust cross-material performance by proposing either novel handcrafted features or utilizing modern deep CNN architectures. There is only up to a three-fold drop in performance by these FPAD methods [4-20]. A summary of the above FPAD model is given in Table 1.

Table 1. Summary of the previously proposed FPAD methods.

Reference	Proposed Method	Category
Rattani et al. [4]	LBP, LPQ, and BSIF features and applied W-SVM	Handcrafted
Ding et al. [5]	LBP, GLCM, BSIF, LPQ, and BGP with One Class SVM	Handcrafted
Yuan et al. [6]	Local Gradient Pattern (LGP) for efficient texture enhancement along with a deep residual network	Hybrid (Handcrafted and Deep learning)
Xia et al. [7]	WLBD	Handcrafted
Sharma et al. [8]	LABP and ULBP texture descriptors	Handcrafted
Sharma et al. [9]	CLBP with LALBP along with eight-layer CNN architecture	Hybrid (Handcrafted and Deep learning)
Nogueira et al. [10]	AlexNet, VGG-19, and LBP (Compared Deep Learning methods with handcrafted methods)	Deep Learning Method
Marasco et al. [11]	CaffeNet, GoogleNet, and Siamese	Deep Learning Method
Park et al. [12]	SqueezeNet-CNN	Deep Learning Method
Pala et al. [13]	TripletNet-CNN	Deep Learning Method
Chugh et al. [14]	Minutiae centered fingerprint patches with Inception v3-based CNN	Deep Learning Method
Zhang et al. [15]	SlimRes CNN based on residual Network	Deep Learning Method
Liu et al. [16]	MobileNet V3	Deep Learning Method
Agarwal et al. [17]	LBP, LPQ, and BSIF with ResNet-50 based CNN model (Incremental Learning)	Hybrid (Handcrafted and Deep learning)
Chugh et. al. [18]	Universal material generator based on VGG-16	Deep Learning Method
Rai et al. [19]	Ensemble network based on MobileNet	Deep Learning Method
Rai et al. [20]	Local Phase Quantization, Frequency Domain Analysis, Ridge-Valley Clarity, Gabor Quality, Orientation Certainty Level, Ridge-Valley Smoothness, and DenseNet-121 ensemble-based model	Hybrid (Handcrafted and Deep learning)

The traditional FPAD methods [4-20] generally extract features from the source dataset while training. When the trained FPAD methods are given a different target dataset (fingerprint from different sensors) while testing, there is a huge drop in performance. As there is variation in extracted features of source and target dataset (domain-shift) from different fingerprint sensors.

III. Proposed Model

To mitigate the domain-shift in source and target dataset this research article has proposed unsupervised domain adaptation (UDDA) for extraction of domain invariant features intended for the FPAD task. The architecture of the UDDA method has been given in Fig. 2. In the suggested method, the divergence between the source and target sensor has been minimized by the use of unsupervised domain adaptation. The model uses labeled input photos from the source sensor and unlabeled fingerprint images from the target sensor to learn sensor-independent features during the training phase. The fingerprint images are scaled to fit CNN. We have utilized the novel

adaptive loss function which uses cross-entropy loss for fingerprint classification along with the domain discrepancy loss to learn the sensor-independent features. In the testing phase, the model takes labeled target sensor fingerprint images for analyzing the cross-sensor generalization performance. The details of each block of the offered method (UDDA) have been given in further subsections.

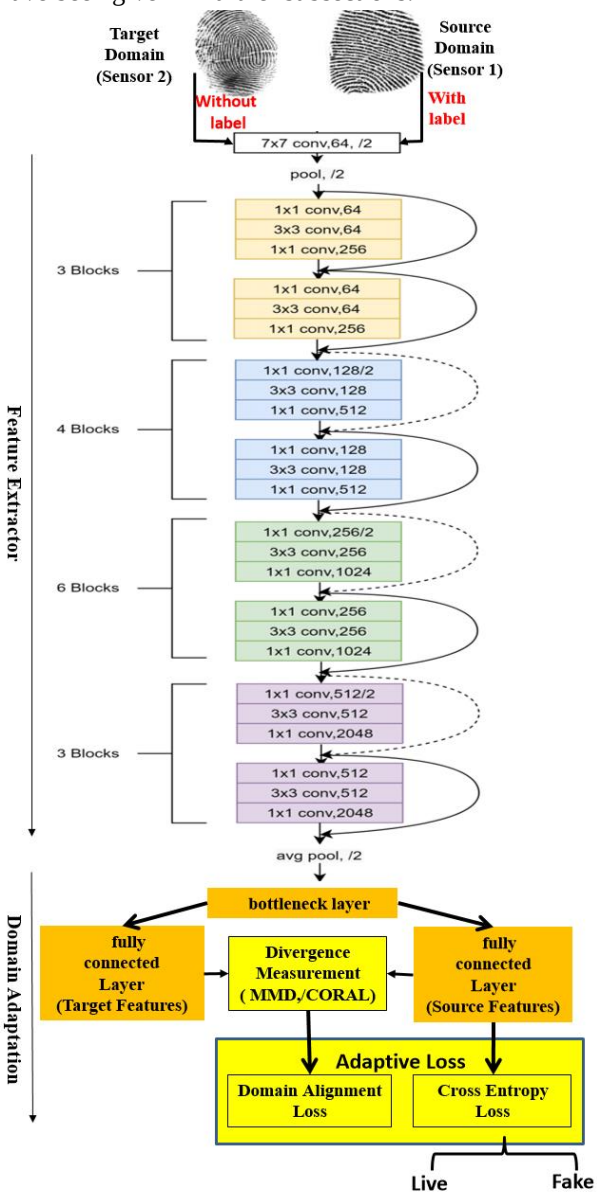

Fig. 2. Proposed unsupervised domain adaptation (UDDA) model for FPAD.

A. Feature Extraction

For feature extraction from the source sensor and target sensor, any CNN architecture can be utilized. In this study, we have utilized ResNet50 [21] as base CNN as it utilizes skip connection and handles vanishing gradient problems effectively. We have modified the fully connected layer (FC) of the original ResNet-50 since we have to categorize the fingerprint images as live or fake (binary classification). We have added a bottleneck layer and an FC layer that utilizes novel ALF to regularize the distribution discrepancy and effective classification of live and fake fingerprints.

B. Unsupervised Domain Adaptation

$$Let \quad D_s = \{(x_i^s, y_i^s)\}_{i=1}^{n_s} \tag{1}$$

Where D_s is the source domain (sensor 1), x_i^s is the i[th] fingerprint image along with its label $y_i^s \in$ {live, fake}, n_s is the number of fingerprint images in the source sensor.

$$D_t = \{(x_j^t)\}_{j=1}^{m_t} \tag{2}$$

Where D_t is the target domain (sensor 2), x_j^t is the jth un-labeled fingerprint image, m_t is the total number of fingerprints in the target sensor, and $m_t <= n_s$. The goal is to learn sensor-independent features by building a classifier that can minimize the cross-sensor generalization error. Let $y = C_\theta$ (x) be an FPAD classifier (outputs labels fake/live), which will minimize the cross-sensor error, then the target sensor error is as follows:

$$\xi_t(\theta) = P_r(x_j^t, y) \sim D_t[C_\theta(x_j^t) \neq y]_{j=1}^{m_t} \tag{3}$$

Equation (3) states that the prediction (P_r) of the classifier is different from the actual label of the fingerprint. To minimize the classification error using source supervisor this study proposes an adaptive loss function (ALF) which is defined in Equation (4).

$$\text{ALF} = \min_\theta \frac{1}{n_l} \sum_{i=1}^{n_l} J(C_\theta(x_i^l), y_i^l) + \lambda d(D_s, D_t) \tag{4}$$

Where $J(C_\theta(x_i^l), y_i^l)$ is the cross entropy loss for classification of fingerprint as live and fake, and $d(D_s, D_t)$ is the domain discrepancy loss which identifies sensor independent features, λ is the hyper-parameter tuned via experiment and l represents the source and target sensor. To minimize the domain discrepancy, we have utilized MMD and CORAL as divergence measurements between the source and target sensor.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

1) Maximum Mean Discrepancy(MMD) Loss

We have utilized MMD loss [2] along with Gaussian kernel to calculate the distribution dissimilarity between source and target sensor; to lessen the domain discrepancy. To ascertain if the two samples are from the same distribution, MMD maps the features to a Hilbert Space with Reproducing Kernel (RKHS) and then compares their means. We have used MMD as it is more robust to noise and small variations in the data as well as it is more flexible due to the use of kernel functions. MMD aligns the distributions by focusing on mean and covariance. Let x_i^s and x_i^t be the two sets of samples from the source sensor (D_s) and the target sensor (D_t), (for simplicity let $m_t = n_s = m$), and $h(x_i^s), h(x_j^s)$ are the extracted features by a CNN(ResNet-50 in our case)'s fully connected layer, then MMD has been calculated using Equation (5) as follows:

$$d_{mmd}^2(D_s, D_t) = \frac{1}{m^2}\left(\sum_{i,j=1}^{m} k(h(x_i^s), h(x_j^s)) + \sum_{i,j=1}^{m} k(h(x_i^t), h(x_j^t)) - 2\sum_{i,j=1}^{m} k(h(x_i^s), h(x_j^t))\right) \tag{5}$$

Where k is the Gaussian kernel function defined using Equation (6).

$$k(h(x_i^s), h(x_j^s)) = e^{-\frac{||h(x_i^s), h(x_j^s)||^2}{2\sigma^2}} \tag{6}$$

2) Correlation Alignment (CORAL) Loss

For comparison, we have exploited CORAL [3] loss for cross-sensor generalization. CORAL matches the source and target distributions' correlations or second-order statistics. Let $C(D_s)$ and $C(D_t)$ be the feature covariance matrices of the source sensor and target domains sensors respectively. Then coral loss is calculated as given in Equation (7).

$$d_{coral}^2(D_s, D_t) = \frac{1}{4d^2}\|C(D_s) - C(D_t)\|_{Fr}^2 \tag{7}$$

Where $\|C(D_s) - C(D_t)\|_{Fr}^2$ is the Frobenius norm and d is the dimensionality of the feature vector. To calculate $C(D_s)$ and $C(D_t)$ we will utilize Equation (8) and Equation (9) given below;

$$C(D_s) = \frac{1}{m-1}\left(d_s^T d_s - \frac{1}{m}(I^T d_s)^T (I^T d_s)\right) \tag{8}$$

$$C(D_t) = \frac{1}{m-1}\left(d_t^T d_t - \frac{1}{m}(I^T d_t)^T (I^T d_t)\right) \tag{9}$$

In Equation (8) and Equation (9), I represent the column vector of 1's. To calculate the gradient of input features by chain rule we will utilize Equation (10) and Equation (11) as given below;

$$\frac{\partial d_{coral}(D_s,D_t)}{\partial d_s^{ij}} = \frac{1}{d^2(m-1)}\left((d_s^T - \frac{1}{m}(I^T d_s)^T I^T)^T (C(D_s) - C(D_t))\right)^{ij} \quad (10)$$

$$\frac{\partial d_{coral}(D_s,D_t)}{\partial d_t^{ij}} = \frac{1}{d^2(m-1)}\left((d_t^T - \frac{1}{m}(I^T d_t)^T I^T)^T (C(D_s) - C(D_t))\right)^{ij} \quad (11)$$

The transpose is denoted by T in equations (10) and (11) and m is the number of fingerprints in each sensor.

IV. Result and Discussion

First, we have discussed the fingerprint datasets used in this study to evaluate the proposed model and then in further subsections given the experimental setup and ablation study.

A. Dataset and Evaluation Metrics

To assess the performance of the UDDA method, we have utilized LivDet 2015 (LD-15) [22] and LivDet 2017 (LD-17) [23] data sets. LivDet 2015 dataset was created to focus on the never-seen-before [24] attacks. In the LivDet 2017 dataset, training, and testing datasets have different material fake fingerprints as given in Table 2.

Table 2. Sensor and materials details used for the creation of fake fingerprints in LD-15 and LD-17 datasets.

Dataset	Fingerprint Sensor	Train Data Set	Test Data Set
LivDet 2015 (LD-15) [22]	Green Bit, Cross-match, Biometrika, and Digital Persona	Body-Double, EcoFlex, Play-Doh, Latex, WoodGlue	Same as the train set with additional fake fingerprints made of OOMOO, Gelatin, and Liquid Ecoflex
LivDet 2017 (LD-17) [23]	Green Bit, Orcanthus, and Digital Persona	Body Double, EcoFlex, and Wood Glue	Latex, Gelatine, and Liquid Ecoflex

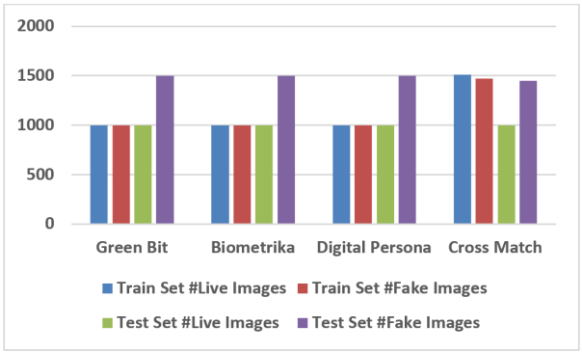

Fig. 3. Distribution of fingerprint images in the LD-15 [22] dataset's train and test sets.

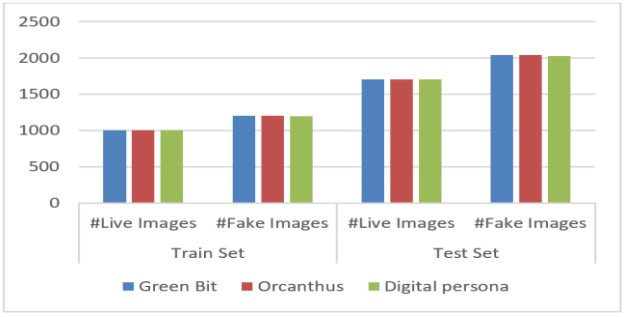

Fig. 4. Distribution of fingerprint images in the LD-17 [23] dataset's train and test sets.

To evaluate the FPAD methods as per the [25] ISO/IEC 30107-3 standards we have utilized Attack Presentation Classification Error Rate (APCER) and Bonafide Presentation Classification Error Rate (BPCER), which denotes the rate of incorrectly categorized attack presentation (fake samples) and misclassified bonafide presentation (live samples) respectively by the PAD system. The classification error (ACE) which is the average of APCER and BPCER is utilized to assess the UDDA, which is calculated using Equation (12).

$$ACE = \frac{APCER+BPCER}{2} \quad (12)$$

Further, ACE can be used to calculate the accuracy (Acc) of the FPAD method using Equation (13).

$$Acc = 100 - ACE \quad (13)$$

B. Experimental setup

The proposed UDDA model utilizes a stochastic gradient descent (sgd) optimizer and uses an adaptive loss function. It consists of cross-entropy loss for fingerprint classification and MMD loss or CORAL loss for domain divergence as given in Equation (4). The rest of the hyper-parameters are used as given in Table 3.

Table 3. Hyper-parameters and their values as used in the experiment.

Hyper-parameters	Value
Learning rate	0.0001
Dropout	0.5
Batch size	32
Epochs	100
λ adaptive loss hyper-parameter	10

All the tests have been accompanied on an Intel Core i5 processor with 16 GB RAM and 4 GB RTX 3050 graphics card memory on the Windows 11 platform.

C. Ablation Study

In the experiment, we analyzed the effectiveness of the ResNet-50 CNN model on the LD-15 dataset without applying the domain adaptation concept in cross-sensor scenarios. The fingerprints from one sensor (like Greenbit) serve as the source domain in this configuration, while the fingerprints from a different sensor (like Digital Persona) serve as the target domain. When fingerprint images come from the same sensor (similar distribution) in both the training and test sets, we have find that the ResNet-50 CNN model performs well and achieves consistent accuracy throughout the train and test datasets. But when the train and test datasets have fingerprint images from different sensors (distribution) the accuracy of the ResNet-50 CNN model degrades drastically (up to 30% reduction in accuracy) as shown in Table (3). The primary cause of this decline in the model's performance is that it was trained only using features from the source sensor dataset. Furthermore, because fingerprint pictures from various sensors have varying textural qualities, the FPAD model performs worse when evaluated on a different test dataset with slightly different features. We have tested the ReNet-50 CNN model on the LD-15 dataset both with and without domain adaptation to get over this restriction.

In the domain adaption scenario, the first fully connected layer of ResNet-50 has been eliminated and substituted with a bottleneck layer and a fully connected layer for fingerprint classification. We have utilized the proposed adaptive loss function (ALF) as given in Equation (4) for identifying the domain invariant features and classification. The proposed FPDA unsupervised domain adaption model (UDDA) uses MMD loss and CORAL loss separately, in the adaptive loss function. From the experiment, we found that MMD loss offers a better reduction in ACE in comparison to CORAL loss (Table 4). MMD loss assesses the difference between distributions without assuming any specific functional forms. It is effective in capturing differences in higher-order statistics besides mean and covariance. Since CORAL anticipates a linear transition across domains and is primarily concerned with matching second-order statistics between source and destination domains, it may perform poorly if the connection is noticeably nonlinear. This is the plausible cause of less degradation in ACE by CORAL loss. So forth we have utilized the MMD loss function for further evaluation of the LD-17 dataset.

Table 4. Classification error (ACE) comparison of the ResNet50 base model on the LD-15 dataset (Note: UDDA is not applicable when training and test datasets come from the same sensor).

Data Set	Training Dataset Sensor	Testing Dataset Sensor	ACE (in %)		
			Without UDDA	With UDDA using MMD	With UDDA using CORAL

		Crossmatch	2.03	-	-
		Digital Persona	4.23	-	-
		Biometrika	4.15	-	-
		Greenbit	2.25	-	-
		Average	***3.16***	**-**	**-**
LD-15 [22]	Crossmatch	Digital Persona	50.82	32.67	35.43
		Biometrika	45.25	28.61	30.25
		Greenbit	44.23	27.01	31.63
	Digital Persona	Crossmatch	33.04	22.92	25.21
		Biometrika	42.28	23.26	24.15
		Greenbit	34.43	17.31	18.19
	Biometrika	Crossmatch	39.52	18.34	18.28
		Digital Persona	23.47	15.26	17.61
		Greenbit	19.91	11.7	15.54
	GreenBit	Crossmatch	32.04	12.9	14.62
		Biometrika	32.97	17.95	19.42
		Digital Persona	20.34	11.45	15.22
		Average	***34.86***	***19.94***	***22.13***

D. Experimental results

The proposed UDDA method which utilizes a novel ALF based on MMD loss or cross-entropy loss is evaluated on the LD-17 dataset for cross-sensor performance evaluation and results were compared with the previously published FPAD methods. In cross-sensor scenario, the results of the UDDA model on the LD-17 dataset have been reported in Table 5.

Table 5: Comparison of the cross-sensor performance of our UDDA model and other FPAD methods on the LD-17 dataset (values are in ACE %).

Data Set	Training DataSet Sensor	Testing Dataset Sensor	Proposed method (UDDA)	Slim-ResCNN [15]	FSB [26]	MoSFPAD [19]	FSB+UMG [18]
LD-17 [23]	GreenBit	Orcanthus	26.64	56.02	50.57	42.67	33.95
		Digital Persona	12.23	19.61	10.63	16.45	5.19
	Orcanthus	GreenBit	17.35	31.18	30.07	27.42	18.25
		Digital Persona	22.12	37.70	42.01	38.71	23.64
	Digital Persona	GreenBit	8.32	12.10	10.46	22.61	3.65

	Orcanthus	28.73	55.70	50.68	41.75	31.56
	Average	***19.23***	***35.39***	***32.40***	***31.60***	***19.37***

The proposed model offers an average ACE of 19.23 on cross-sensor evaluation on the LD-17 dataset, which is substantially less than other FPAD approaches [15] [18] [26] and [19].

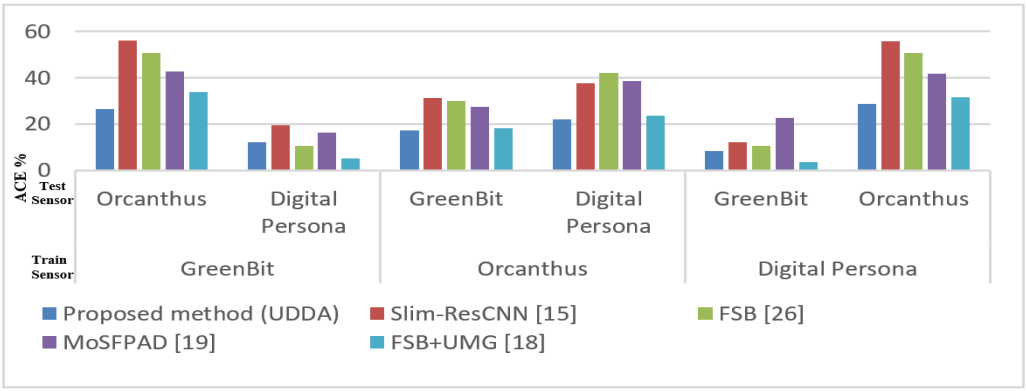

Figure 5. Comparison of ACE (%) of proposed UDDA and other FPAD methods on LD-17 dataset.

Our UDDA method perform identical to the state-of-the-art FPAD method provided by Chugh et al. [18]. Their FPAD method [18] have used a universal material generator to enhance the performance of the current FPAD model, which focuses on producing the texture of unseen fake material. The UMG-based model is computationally expensive because it generates the novel fingerprint patches first, and then learns over them. The proposed UDDA model offers the least or almost similar (in some cases) ACE value because it learns the domain invariant features instead of generating the common set of features of source and target domains (which is computationally expensive) [18].

V. Conclusion

Despite the tremendous growth in the FPAD methods, most of the methods fail to generalize in cross-sensor scenarios. This is mostly because these techniques are trained on sensor-dependent features. This paper suggests a novel FPDA approach (UDDA) that makes use of a special adaptive loss function for a resilient FPAD method. It aids in the learning of domain-invariant features for any basic CNN model by combining the cross-entropy loss and MMD loss. Two LivDet datasets that are available to the public have been used to evaluate the suggested model (UDDA). The outcomes of the study demonstrate that unsupervised domain adaptation contributes to an improvement in cross-sensor generalization ability.

References

[1] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition (Vol. 2). London: springer.

[2] Long, M., Cao, Y., Wang, J., & Jordan, M. (2015, June). Learning transferable features with deep adaptation networks. In International conference on machine learning (pp. 97-105). PMLR.

[3] Sun, B., & Saenko, K. (2016). Deep coral: Correlation alignment for deep domain adaptation. In Computer Vision–ECCV 2016 Workshops: Amsterdam, The Netherlands, October 8-10 and 15-16, 2016, Proceedings, Part III 14 (pp. 443-450). Springer International Publishing.

[4] Rattani, A., Scheirer, W. J., & Ross, A. (2015). Open set fingerprint spoof detection across novel fabrication materials. IEEE Transactions on Information Forensics and Security, 10(11), 2447-2460.

[5] Ding, Y., & Ross, A. (2016, December). An ensemble of one-class SVMs for fingerprint spoof detection across different fabrication materials. In 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (pp. 1-6). IEEE.

[6] Yuan, C., Xia, Z., Sun, X., & Wu, Q. J. (2019). Deep residual network with adaptive learning framework for fingerprint liveness detection. IEEE Transactions on Cognitive and Developmental Systems, 12(3), 461-473.

[7] Xia, Z., Yuan, C., Lv, R., Sun, X., Xiong, N. N., & Shi, Y. Q. (2018). A novel Weber local binary descriptor for fingerprint liveness detection. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(4), 1526-1536.

[8] Sharma, D., & Selwal, A. (2022). An intelligent approach for fingerprint presentation attack detection using ensemble learning with improved local image features. Multimedia Tools and Applications, 81(16), 22129-22161.

[9] Sharma, D., & Selwal, A. (2022). HyFiPAD: a hybrid approach for fingerprint presentation attack detection using local and adaptive image features. The Visual Computer, 38(8), 2999-3025.

[10] Nogueira, R. F., de Alencar Lotufo, R., & Machado, R. C. (2016). Fingerprint liveness detection using convolutional neural networks. IEEE transactions on information forensics and security, 11(6), 1206-1213.

[11] Marasco, E., Wild, P., & Cukic, B. (2016, May). Robust and interoperable fingerprint spoof detection via convolutional neural networks. In 2016 IEEE symposium on technologies for homeland security (HST) (pp. 1-6). IEEE.

[12] Park, E., Cui, X., Kim, W., Liu, J., & Kim, H. (2018). Patch-based fake fingerprint detection using a fully convolutional neural network with a small number of parameters and an optimal threshold. arXiv preprint arXiv:1803.07817.

[13] Pala, F., & Bhanu, B. (2017). Deep triplet embedding representations for liveness detection. Deep learning for biometrics, 287-307.

[14] Chugh, T., Cao, K., & Jain, A. K. (2017, October). Fingerprint spoof detection using minutiae-based local patches. In 2017 IEEE International Joint Conference on Biometrics (IJCB) (pp. 581-589). IEEE.

[15] Zhang, Y., Shi, D., Zhan, X., Cao, D., Zhu, K., & Li, Z. (2019). Slim-ResCNN: A deep residual convolutional neural network for fingerprint liveness detection. IEEE Access, 7, 91476-91487.

[16] Liu, H., Zhang, W., Liu, F., Wu, H., & Shen, L. (2021). Fingerprint presentation attack detector using global-local model. IEEE Transactions on Cybernetics, 52(11), 12315-12328.

[17] Agarwal, S., Rattani, A., & Chowdary, C. R. (2022). A-iLearn: An adaptive incremental learning model for spoof fingerprint detection. Machine Learning with Applications, 7, 100210.

[18] Chugh, T., & Jain, A. K. (2020). Fingerprint spoof detector generalization. IEEE Transactions on Information Forensics and Security, 16, 42-55.

[19] Rai, A., Dey, S., Patidar, P., & Rai, P. (2023). Mosfpad: an end-to-end ensemble of mobile net and support vector classifier for fingerprint presentation attack detection. arXiv preprint arXiv:2303.01465.

[20] Rai, A., Tiwari, P. K., Baishya, J., Sharma, R. P., & Dey, S. (2023). DyFFPAD: Dynamic Fusion of Convolutional and Handcrafted Features for Fingerprint Presentation Attack Detection. arXiv preprint arXiv:2308.10015.

[21] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 770-778).

[22] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), Arlington, VA, USA, 2015, pp. 1-6.

[23] Mura, V., Orrù, G., Casula, R., Sibiriu, A., Loi, G., Tuveri, P., ... & Marcialis, G. L. (2018, February). LivDet 2017 fingerprint liveness detection competition 2017. In 2018 international conference on biometrics (ICB) (pp. 297-302). IEEE.

[24] Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L., & Schuckers, S. (2023). Review of the Fingerprint Liveness Detection (LivDet) competition series: from 2009 to 2021. Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment, 57-76.

[25] ISO/IEC 30107-3:2023(en) Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. Available online at: https://www.iso.org/standard/79520.html. (accessed on 21 December 2023)

[26] Chugh, T., & Jain, A. K. (2019, June). Fingerprint presentation attack detection: Generalization and efficiency. In 2019 International Conference on Biometrics (ICB) (pp. 1-8). IEEE.

[27] ISO/IEC 30107-1:2023(en) Information technology — Biometric presentation attack detection — Part 1: Framework. Available online at: https://www.iso.org/standard/83828.html. (accessed on 21 December 2023).

[28] Uludag, U., & Jain, A. K. (2004, June). Attacks on biometric systems: a case study in fingerprints. In Security, steganography, and watermarking of multimedia contents VI (Vol. 5306, pp. 622-633). SPIE.

[29] Grosz, S. A., Chugh, T., & Jain, A. K. (2020, September). Fingerprint presentation attack detection: A sensor and material agnostic approach. In 2020 IEEE international joint conference on biometrics (IJCB) (pp. 1-10). IEEE.

[30] Karampidis, K., Rousouliotis, M., Linardos, E., & Kavallieratou, E. (2021). A comprehensive survey of fingerprint presentation attack detection. Journal of Surveillance, Security and Safety, 2(4), 117-161.

[31] Micheletto, M., Orrù, G., Casula, R., & Marcialis, G. L. (2022). Mitigating Sensor and Acquisition Method-Dependence of Fingerprint Presentation Attack Detection Systems by Exploiting Data from Multiple Devices. Applied Sciences, 12(19), 9941.