A robust fingerprint presentation attack detection method against unseen attacks through adversarial learning

Joao Afonso Pereira[1], Ana F. Sequeira[1], Diogo Pernes[1,2], Jaime S. Cardoso[1,3]

Abstract: Fingerprint presentation attack detection (PAD) methods present a stunning performance in current literature. However, the *fingerprint PAD generalisation problem* is still an open challenge requiring the development of methods able to cope with sophisticated and unseen attacks as our eventual intruders become more capable. This work addresses this problem by applying a regularisation technique based on an adversarial training and representation learning specifically designed to to improve the PAD generalisation capacity of the model to an unseen attack. In the adopted approach, the model jointly learns the representation and the classifier from the data, while explicitly imposing invariance in the high-level representations regarding the type of attacks for a robust PAD. The application of the adversarial training methodology is evaluated in two different scenarios: i) a handcrafted feature extraction method combined with a Multilayer Perceptron (MLP); and ii) an end-to-end solution using a Convolutional Neural Network (CNN). The experimental results demonstrated that the adopted regularisation strategies equipped the neural networks with increased PAD robustness. The adversarial approach particularly improved the CNN models' capacity for attacks detection in the unseen-attack scenario, showing remarkable improved APCER error rates when compared to state-of-the-art methods in similar conditions.

Keywords: Fingerprint presentation attack detection, adversarial learning, transfer learning.

1 Introduction

Biometric recognition is nowadays a mature technology used in many government and civilian applications such as e-passports, ID cards, border control and in most of unlock/authentication systems present in handheld devices. Fingerprint recognition systems (FRS) in particular are widely used probably having been this the first biometric trait used to identify people. Fingerprint presentation attack detection (FPAD) methods have been developed as an attempt to overcome the vulnerability of FRS to spoofing. However, most of the traditional approaches have been quite optimistic about the behavior of the intruder, assuming the use of a previously known type of attack sample. This assumption has led to the overestimation of the performance of the methods, using both live and spoof samples to train the predictive models and evaluate each type of fake samples individually [SC15].

The presentation attack detection (PAD) generalisation capacity of a model to unseen attacks, has been addressed before regarding iris, fingerprint and face. However, it still remains a challenging topic. Whether in research or deployment of PAD systems in commercial applications, if the classification models are designed and evaluated using bona fide presentations and presentation attack instruments (PAI) belonging only to specific species

[1] INESC TEC, Porto, Portugal, Email: {joao.a.pereira,ana.f.sequeira, diogo.pernes, jaime.cardoso}@inesctec.pt

[2] Faculdade de Ciencias da Universidade do Porto, Porto, Portugal

[3] Faculdade de Engenharia da Universidade do Porto, Porto, Portugal

(PAISp), then the case when the model is confronted with a PAISp which is significantly different from the ones used for training is overlooked. In the worst case scenario, such sample may have higher probability to circumvent the system than the ones drawn from the original training dataset and the model may fail to generalise robustly and detect the threat. To solve this research question is necessary to develop robust methods to cope with sophisticated and unseen attacks as our eventual intruders become more capable and successfully develop new spoofing techniques.

The pioneer work in the evaluation of PAD methods across different types and unseen PAISp appeared in the fingerprint domain with the work of Marasco and Sansone [MS11]. The works of Rattani & Ross [RSR15] and Sequeira & Cardoso [SC15], despite using different approaches, both relied on the idea of enforcing the knowledge of the bona fide (BF) presentations over the presentation attack (PA) to better deal with unseen PAISp. With the rise of deep learning (DL) techniques, PAD methods based on deep representations were proposed using the binary approach [Me15, Pi18]. Followed by works tackling DL fingerprint PAD methods robustness to unseen PAISp. In [To18], was proposed a highly accurate method based on CNNs and own multi-spectral short wave infrared imaging. The LivDet competition series in 2015 [Mu15] included evaluation with unseen attacks, however unfortunately this scenario was not tested in following editions. The PAD generalisation problem has been addressed regarding other biometric traits. Regarding iris, Sequeira *et al* [Se16] stated that whenever a new PAISp is presented in the test step, the performance of the classifier drops and improvement can be obtained using BF one-class classification; and in [Fe19a] a successful adversarial strategy is proposed. Nevertheless, most of the recent approaches, either make overly optimistic assumptions about the attacker - binary classification approaches - or only use part of the data (and therefore, of the knowledge) available at training time to design the models - one-class approaches. Alternatively, the approach evaluated in this work uses the information of both BF and known PA and is robust to unseen PAI species.

In this work, the *FPAD generalisation problem* is addressed by means of a regularisation technique applied to artificial neural networks combining adversarial training with representation learning. In this approach, designed to improve the generalisation capacity to unseen attacks, the proposed model jointly learns the representation and the classifier from the data, while explicitly imposing ‘PAI-species’-invariance in the high-level representations for a robust PAD method. The algorithm applied here was presented by Ferreira *et al* [Fe19b] in the context of sign language recognition, with a later application to iris PAD [Fe19a]. This approach builds on those initially introduced by Ganin *et al* [GL15], for domain adaptation, and Feutry *et al* [Fe18], to learn anonymized representations.

The contributions of this work are then two-fold: 1) the application of the adversarial training concept to the generalisation to unseen attacks problem in fingerprint PAD; and 2) the evaluation of the adversarial training methodology in two different scenarios: i) a handcrafted feature extraction method combined with a Multilayer Perceptron (MLP); ii) an end-to-end solution using a Convolutional Neural Network (CNN).

The main definitions related to PAD concepts used throughout this paper are the ones stated in the International Standard ISO/IEC 30107-3 Information Technology — Biometric presentation attack detection — Part 3: Testing and reporting [IS17].

This paper is organised as follows. This section summarises the related and proposed work and how it addresses the research question posed. In section 2 the methodology used is detailed. Section 3 describes the experimental setup including the results and discussion. Section 4 concludes the work with the final remarks.

2 Methodology

This section summarises the methodology from Ferreira *et al* [Fe19a], which is adopted here with the appropriate adjustments. The underlying idea behind this approach is that, in order to generalise well to unseen attacks, the model should not specialize in discriminating any of the PAI species (PAISp) presented at training time and, therefore, the learned internal representations should be invariant to the PAISp. For this purpose, the model combines an adversarial approach with a species-transfer training objective, which are described in the remaining of the section. The high-level architecture of the model is summarized in Figure 1. Throughout this section, it should be assumed that one has access to a labeled dataset $\mathbb{X} = \{\boldsymbol{X}_i, y_i, s_i\}_{i=1}^{N}$ of N samples, where $\boldsymbol{X}_i$ represents the i-th input sample, and y_i and s_i denote the corresponding class label (*bona fide* or *attack*) and the PAI species (only defined for attack samples), respectively. Let $\mathbb{X}^{bf}$ and $\mathbb{X}^{a}$ be these partitions of $\mathbb{X}$ for bona-fide and attack samples, respectively, and N^{bf} and N^{a} their respective cardinality.

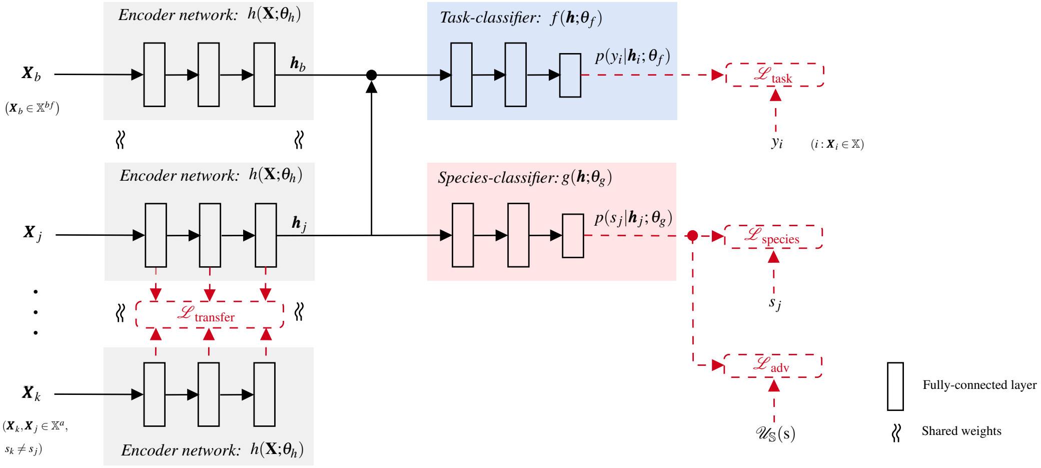
Encoder network: $h(\mathbf{X};\theta_h)$
$\boldsymbol{X}_b$
$(\boldsymbol{X}_b \in \mathbb{X}^{bf})$
$\boldsymbol{h}_b$
Task-classifier: $f(\boldsymbol{h};\theta_f)$
$p(y_i|\boldsymbol{h}_i;\theta_f)$
$\mathscr{L}_{\text{task}}$
y_i
$(i : \boldsymbol{X}_i \in \mathbb{X})$
Encoder network: $h(\mathbf{X};\theta_h)$
$\boldsymbol{X}_j$
$\boldsymbol{h}_j$
Species-classifier: $g(\boldsymbol{h};\theta_g)$
$p(s_j|\boldsymbol{h}_j;\theta_g)$
$\mathscr{L}_{\text{species}}$
s_j
$\mathscr{L}_{\text{transfer}}$
$\boldsymbol{X}_k$
$(\boldsymbol{X}_k, \boldsymbol{X}_j \in \mathbb{X}^a,$
$s_k \neq s_j)$
Encoder network: $h(\mathbf{X};\theta_h)$
$\mathscr{L}_{\text{adv}}$
$\mathscr{U}_{\mathbb{S}}(\mathrm{s})$
Fully-connected layer
Shared weights

Fig. 1: The architecture of the proposed species-invariant neural network (from [Fe19a]).

2.1 Adversarial learning

The model comprises three main sub-networks: (i) an encoder network $h(\cdot;\theta_h)$ that receives input samples and maps them to a latent space; (ii) a *task-classifier* network $f(\cdot;\theta_f)$ which aims to distinguish attack and bona fide samples, mapping latent representations to the corresponding class probabilities; and (iii) a *species-classifier* network $g(\cdot;\theta_g)$ that receives latent representations from attack samples and aims to predict the corresponding

PAI species. In order to learn 'PAI-species'-invariant latent representations, an adversarial learning scheme is adopted. The species-classifier is trained to minimize the classification loss of the PAI-species:

$$\min_{\theta_g} \mathscr{L}_{\text{species}}(\theta_h, \theta_g) = \min_{\theta_g} \left\{ -\frac{1}{N^a} \sum_{i=1}^{N^a} \log p(s_i | h(\boldsymbol{X}_i; \theta_h); \theta_g) \right\}, \ \boldsymbol{X}_i \in \mathbb{X}^a. \tag{1}$$

Simultaneously, the task-classifier and the encoder are jointly trained to minimize the classification loss between attacks and bona fide samples, while trying to keep the PAI-species classification close to random guessing (i.e., close to a uniform distribution):

$$\min_{\theta_h, \theta_f} \mathscr{L}(\theta_h, \theta_f, \theta_g) = \min_{\theta_h, \theta_f} \left\{ \mathscr{L}_{\text{task}}(\theta_h, \theta_f) + \lambda \mathscr{L}_{\text{adv}}(\theta_h, \theta_g) \right\}, \tag{2}$$

where

$$\mathscr{L}_{\text{task}}(\theta_h, \theta_f) = -\frac{1}{N} \sum_{i=1}^{N} \log p(y_i | h(\boldsymbol{X}_i; \theta_h); \theta_f), \tag{3}$$

$$\mathscr{L}_{\text{adv}}(\theta_h, \theta_g) = \frac{1}{N^a} \sum_{i=1}^{N^a} D_{\text{KL}}(\mathscr{U}_{\mathbb{S}}(\text{s}) || p(\text{s} | h(\boldsymbol{X}_i; \theta_h); \theta_g), \ \boldsymbol{X}_i \in \mathbb{X}^a. \tag{4}$$

Here, $\mathscr{U}_{\mathbb{S}}$ denotes a uniform distribution over the set of PAI-species present in the training set.

2.2 Species-transfer objective

In addition to the adversarial training, a species-transfer objective is employed to further encourage the latent representations to be species-invariant. This objective enforces the means of the latent representations of different species to coincide. Therefore, this is a weaker constraint than the one imposed by the adversarial objective, but it has a beneficial effect by speeding up the convergence to invariant representations.

Specifically, a layer-wise loss $\mathscr{D}^{(m)}$ between the hidden representations $h^{(m)}(\cdot; \theta_h)$ of two species s and t at the output of the m-th layer of the encoder is defined as:

$$\mathscr{D}^{(m)}(s,t;\theta_h) = \left|\left| \frac{1}{N_s} \sum_{i:\ s_i=s} h^{(m)}(\boldsymbol{X}_i; \theta_h) - \frac{1}{N_t} \sum_{j:\ s_j=t} h^{(m)}(\boldsymbol{X}_j; \theta_h) \right|\right|_2^2, \tag{5}$$

where $|| \cdot ||_2$ is the ℓ^2-norm, and N_s and N_t denote the number of training examples of species s and t, respectively. The overall species-transfer loss $\mathscr{L}_{\text{transfer}}$ is then a weighted sum of the losses computed at each layer of the *encoder* network:

$$\mathscr{L}_{\text{transfer}}(\theta_h) = \sum_{m=1}^{M} \beta^{(m)} \mathscr{L}_{\text{transfer}}^{(m)}(\theta_h) = \sum_{m=1}^{M} \beta^{(m)} \sum_{s \in \mathbb{S}} \sum_{\substack{t \in \mathbb{S}, \\ t \neq s}} \mathscr{D}^{(m)}(s,t;\theta_h), \tag{6}$$

where $\beta^{(m)} \geq 0$ is a hyperparameter that controls the relative importance of the loss obtained at the m-th layer and the species-transfer loss at the m-th layer is the sum of the pairwise distances between all PAISp.

The overall objective function of the encoder and task classifier is then the combination of equations (2) and (6):

$$\min_{\theta_h,\theta_f} \mathscr{L}(\theta_h,\theta_f,\theta_g) = \min_{\theta_h,\theta_f} \left\{ \mathscr{L}_{\text{task}}(\theta_h,\theta_f) + \lambda \mathscr{L}_{\text{adv}}(\theta_h,\theta_g) + \gamma \mathscr{L}_{\text{transfer}}(\theta_h) \right\}, \quad (7)$$

where $\gamma \geq 0$ is the weight that controls the relative importance of the species-transfer term. The objective for the species-classifier remains unchanged, i.e. as in equation (1).

3 Experimental setup

PAD Performance Evaluation Metrics: The *Attack Presentation Classification Error Rate* (APCER) and the *Bona-fide Presentation Classification Error Rate* (BPCER) for an APCER of 5% (*BPCER@APCER=5%*) as defined in the ISO/IEC 30107-3 [IS17]. The Equal Error Rate (EER) analyses the distributions of the APCER and BPCER and corresponds to the minimum value where both are equal.

Dataset: The Fingerprint Liveness Detection Competition 2015 (LivDet2015) [Mu15] training dataset comprises a set of five subsets, each one corresponding to a specific fingerprint sensor. For each sensor there are bona fide samples and different types of PAI.

Evaluation protocols: The adopted framework is denominated “unseen-attack”, as the presentation attack instrument seen in the testing phase is unknown to the model. Thus, the methods are evaluated by saving one type of attack - PAI species - for testing while the training is done with the remaining presentation attack instruments and bona fide samples.

Handcrafted feature extraction method: The extracted features that served as input for the MLP were the histogram of intensity, the histogram of the Local Binary Patterns (LBP) [OPM02] and the histogram of the Local Phase Quantization [OH08].

Implementation details: The models were implemented in Python with the PyTorch library. The training phase was conducted with the Adam optimizer and a batch size of 16. The learning rate and the ℓ^2 regularization weight were both set to 1e^{-04}. The hyperparameters λ and γ, specific to the adopted regularization, were optimized through a grid search and cross-validation on the training dataset, varying on logaritmic scale in the interval [1e^{-03},1]. The $\mathscr{L}_{\text{transfer}}$ penalty is applied to the last layer of the encoder network. Regarding the architecture of the MLP, the encoder corresponds to [(FC(128) →ReLU) x 3] and the classifiers also to [(FC(128) →ReLU) x 3], where FC(n) notes a fully connected layer with n neurons. For the CNN model, the encoder corresponds to [(C(64) →ReLU) x 2 →MaxPool →(C(128) →ReLU) x 2 →MaxPool →(C(256) →ReLU) x 4], where C(f) notes a convolutional layer with f filters, kernel 3x3, stride 1 and padding 1. The CNN's classifiers both correspond to [(FC(4096) →ReLU) x 2 →(FC(1000) →ReLU)].

Results and discussion: In Table 2, the results of the baseline methods (*MLP* and *CNN*) and their respective regularised versions (*MLP$_{reg}$* and *CNN$_{reg}$*) are displayed. Comparing the performance of the baseline and regularised versions, it can be observed that: i) regarding the MLP, except for the Hi Scan sensor, in all the cases there is a significant improvement in at least 2 out of the 3 presented metrics; and ii) regarding the CNN, there is a significant improvement without exception in all error rates, with a particular significant improvement of the APCER value from 4.12% to 0.81% (for the average of the five sensors). From these observations, it can be stated with confidence that, overall, the regularisation technique improves the PAD robustness of both the models.

Still, it is arguable that the performance of the MLP, even the baseline version, outperforms the CNN results. Nevertheless, it should be noted that: i) the first scenario is taking advantage of rich handcrafted features; and ii) the data available for training is not enough to take the best out of the CNN learning capabilities. Thus, on the one hand the end-to-end solution provided by the CNN saves a considerable effort in the computation of the feature extraction step and, on the other hand, increasing the amount of training data will certainly increase the performance of these models, as there is a high potential for growth.

Tab. 1: Baseline and proposed regularised approaches - Cross Match, Digital Persona and Green Bit sensors. ($BPCER@APCER = 5\%$ noted by $BPCER@5$.)

Method	**PAD metrics (%)**								
	Cross Match			*Digital Persona*			*GreenBit*		
	APCER	BPCER@5	EER	APCER	BPCER@5	EER	APCER	BPCER@5	EER
MLP	**0.07**	7.57	4.33	0.00	0.53	0.45	**0.70**	**0.20**	1.10
MLPreg	0.13	**4.30**	**3.70**	**0.00**	**0.00**	**0.30**	**0.70**	0.63	**0.93**
CNN	5.00	6.25	8.70	5.60	10.80	7.28	3.03	14.13	7.05
CNNreg	**1.07**	**4.65**	**2.82**	**0.60**	**3.85**	**2.45**	**0.60**	**2.93**	**1.63**

Tab. 2: Baseline and proposed regularised approaches - Hi Scan and Time Series sensors, as well as the average of the results for the 5 sensors. ($BPCER@APCER = 5\%$ noted by $BPCER@5$.)

Method	**PAD metrics (%)**								
	Hi Scan			*Time Series*			Average of the 5 sensors		
	APCER	BPCER@5	EER	APCER	BPCER@5	EER	APCER	BPCER@5	EER
MLP	**0.30**	**2.83**	**3.03**	**0.00**	**0.03**	0.60	**0.21**	2.23	1.90
MLPreg	1.30	3.60	3.38	**0.00**	**0.03**	**0.10**	0.43	**1.71**	**1.68**
CNN	5.60	20.15	11.25	1.37	9.10	4.07	4.12	12.09	7.67
CNNreg	**1.20**	**1.21**	**1.04**	**0.60**	**6.30**	**2.70**	**0.81**	**3.79**	**2.13**

Despite the evidences showed in favour of the effectiveness of the regularisation technique, it is crucial to compare the results obtained with the proposed approach against the current state-of-the-art DL based PAD that tackle the unseen-attack scenario. This is not an easy task as most works still opt for a more traditional approach, based on binary classification limited to one type of attack at a time. From the available literature using similar databases and addressing the generalisation problem, stands out the meritory initiative of Fingerprint LivDet2015 of evaluating the methods with some unseen types of PAISp.

Table 3 presents the results of the proposed regularised CNN version, *CNNreg*, alongside with the comparable literature methods currently available. The comparison is made with the best results from the LivDet2015 [Gh17, Mu15] for common subsets of the used database, as well as with an additional recent publication [Pa19]. From the observed results, it is remarked the significant improvement of the *CNNreg* in two out of three sensors and undoubtedly when considering the average values. In particular, the *CNNreg* provided an APCER value of 0.76% against 2.09% and 6.33% of the other methods (for the average of the three sensors).

Tab. 3: Literature and proposed approach.($BPCER@APCER = 5\%$ noted by $BPCER@5$.)

Method	**PAD metrics (%)**							
	Cross Match		*Digital Persona*		*GreenBit*		Average	
	APCER	BPCER@5	APCER	BPCER@5	APCER	BPCER@5	APCER	BPCER@5
Proposed CNNreg	1.07	4.65	**0.60**	**3.85**	**0.60**	**2.93**	**0.76**	**3.81**
LivDet2015 [Gh17, Mu15]	1.68	≈ **0.80**	**0.60**	≈ 10.00	4.00	≈ 5.00	2.09	≈ 5.27
Park et al [Pa19]	**0.00**	-	11.00	-	8.00	-	6.33	-

4 Conclusions

This work addresses the *fingerprint PAD generalisation problem* through an adversarial training objective which combines representation learning and artificial neural networks. The method is specifically designed to address the generalisation capacity to an unseen attack by enforcing the learning of the task of distinguishing the bona fide from the attack presentations while ensuring the invariance between the different type of the PAI species.

Comparing the baseline and regularised versions, it can be stated that, overall, the regularisation technique improves the PAD robustness of both the models. Despite the fact that the *MLPreg* fed with rich handcrafted features proved to be competitive, the fact is that *CNNreg* has more potential for growth and for increasing its performance in the future.

The comparison of the proposed approach against the current DL based PAD methods that tackle the unseen-attack scenario, is not an easy task as most works still opt for a more traditional approach based on binary classification limited to one type of attack at a time. Still, from the comparison with the available literature using similar databases and addressing the generalisation problem, it is verified a significant superiority of the *CNNreg* in two out of three sensors and undoubtedly when considering the average values.

Acknowledgements

This work is financed by National Funds through the Portuguese funding agency, FCT - Fundação para a Ciência e a Tecnologia, within project UIDB/50014/2020 and by Ph.D. Grant SFRH/BD/129600/2017.

References

[Fe18] Feutry, Clément; Piantanida, Pablo; Bengio, Yoshua; Duhamel, Pierre: Learning anonymized representations with adversarial neural networks. arXiv:1802.09386, 2018.

[Fe19a] Ferreira, Pedro; Sequeira, Ana Filipa; Pernes, Diogo; Rebelo, Ana; Cardoso, Jaime S.: Adversarial learning for a robust iris presentation attack detection method against unseen attack presentations. In: Proceedings of the 18th BIOSIG. 2019.

[Fe19b] Ferreira, Pedro M.; Pernes, Diogo; Rebelo, Ana; Cardoso, Jaime S.: Learning signer invariant representations with adversarial training. In: 12th ICMV. 2019.

[Gh17] Ghiani, Luca; Yambay, David A.; Mura, Valerio; Marcialis, Gian Luca; Roli, Fabio; Schuckers, Stephanie A.: Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. Image and Vision Computing, 58:110 – 128, 2017.

[GL15] Ganin, Yaroslav; Lempitsky, Victor: Unsupervised Domain Adaptation by Backpropagation. In: Proc. 32nd Int. Conf. ML. volume 37, Lille, France, pp. 1180–1189, 2015.

[IS17] ISO/IEC JTC1 SC37: Information Technology - Biometrics - Presentation attack detection Part 3: Testing and Reporting. ISO Int. Organization for Standardization, 2017.

[Me15] Menotti, D.; Chiachia, G.; Pinto, A.; Robson Schwartz, W.; Pedrini, H.; Xavier Falcao, A.; Rocha, A.: DeepRep.Iris,Face,and Fingerp.Spoof.Det. TIFS, 10(4):864–879, 2015.

[MS11] Marasco, Emanuela; Sansone, Carlo: On the Robustness of Fingerprint Liveness Detect. Alg. against New Materials used for Spoofing. In: BIOSIGNALS. pp. 553–558, 2011.

[Mu15] Mura, Valerio; Ghiani, Luca; Marcialis, Gian; Roli, Fabio; Yambay, David; Schuckers; Schuckers, Stephanie: LivDet2015-Fingerprint Liveness Detect. Competition. 09 2015.

[OH08] Ojansivu, Ville; Heikkilä, Janne: Blur Insensitive Texture Classification Using Local Phase Quantization. In (Elmoataz, Abderrahim; Lezoray, Olivier; Nouboud, Fathallah; Mammass, Driss, eds): Image and Signal Processing. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 236–243, 2008.

[OPM02] Ojala, T.; Pietikainen, M.; Maenpaa, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(7):971–987, July 2002.

[Pa19] Park, E.; Cui, X.; Nguyen, T. H. B.; Kim, H.: Presentation Attack Detection Using a Tiny Fully Convolutional Network. IEEE Transactions on Information Forensics and Security, 14(11):3016–3025, 2019.

[Pi18] Pinto, Allan; Pedrini, Helio; Krumdick, Michael; Becker, Benedict; Czajka, Adam; Bowyer, Kevin W; Rocha, Anderson: Counteracting presentation attacks in face, fingerprint, and iris recognition. Deep Learning in Biometrics, 245, 2018.

[RSR15] Rattani, A.; Scheirer, W.J.; Ross, A.: Open Set Fingerprint Spoof Detection Across Novel Fabrication Materials. IEEE TIFS, 10(11):2447–2460, Nov 2015.

[SC15] Sequeira, Ana F.; Cardoso, Jaime S.: Fingerprint liveness detection in the presence of capable intruders. Sensors, 15:14615–14638, 2015.

[Se16] Sequeira, A. F.; Thavalengal, S.; Ferryman, J.; Corcoran, P.; Cardoso, J. S.: A realistic evaluation of iris presentation attack detection. In: 39th TSP. pp. 660–664, June 2016.

[To18] Tolosana, Ruben; Gomez-Barrero, Marta; Kolberg, Jascha; Morales, Aythami; Busch, Christoph; Ortega-Garcia, Javier: Towards fingerprint PAD based on cnn and short wave infrared imaging. In: 2018 BIOSIG. IEEE, pp. 1–5, 2018.