INESCTEC

Adversarial learning for a robust fingerprint presentation attack detection method against unseen attacks

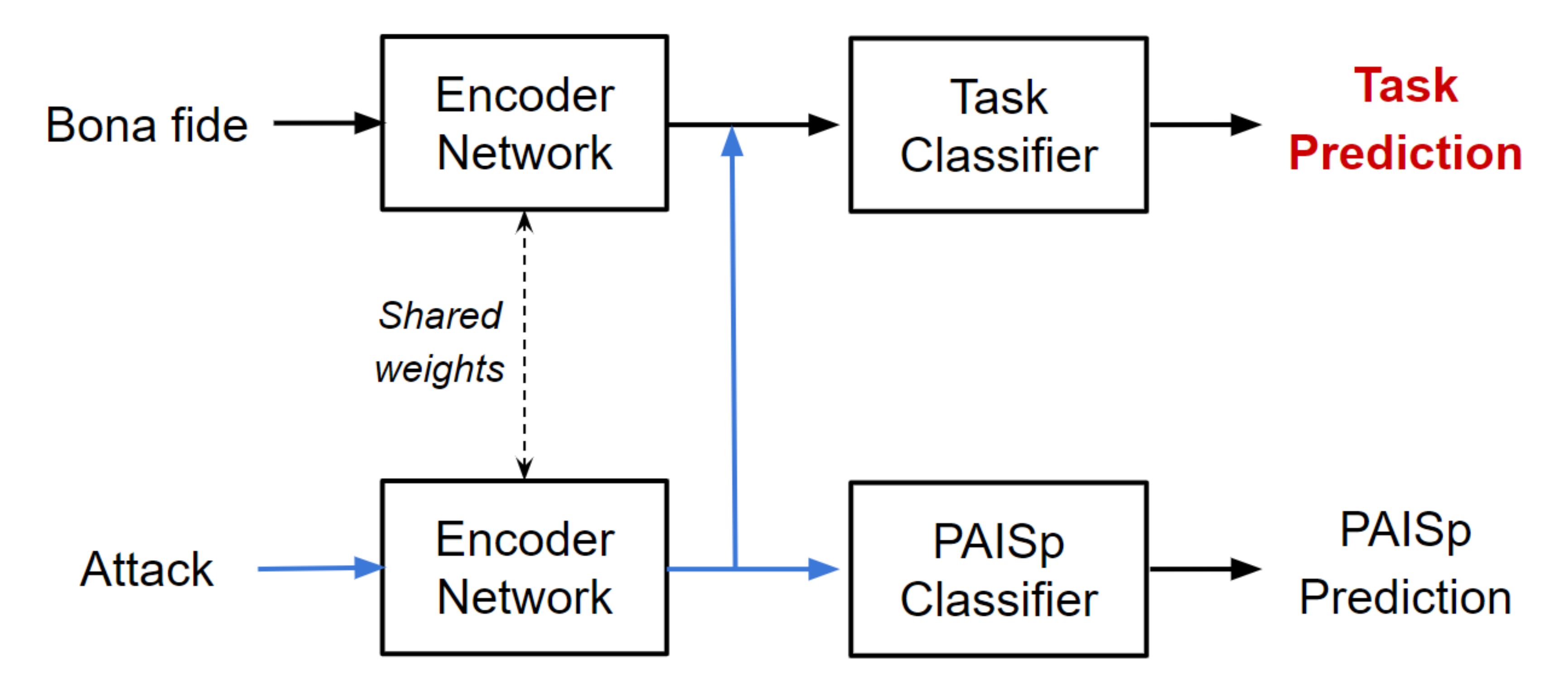
João Afonso Pereira [1] | Diogo Pernes [1,2] | Ana F. Sequeira [1] | Jaime S. Cardoso [1,3]

Overview

This work addresses the problem of unknown fingerprint presentation attacks by applying a regularization technique based on an adversarial training and representation learning specifically designed to improve the presentation attack detection (PAD) generalization capacity of the model to any type of 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.

Methodology

The Encoder Network tries to generate representations that worsen the performance of the PAISp Classifier but that are at the same time good for the Task Classifier, theoretically leading to a more general model that is less dependent on the PAISp and, consequently, more robust to unknown attacks.



$$\boxed{\mathcal{L} = \min\{\mathcal{L}_{Task} + \lambda\mathcal{L}_{Adversarial(PAISp)} + \gamma\mathcal{L}_{Transfer}\}}$$

$\mathcal{L}_{Task}$ corresponds to the loss function of the presentation attack classification task. $\mathcal{L}_{Adversarial(PAISp)}$ enforces the fake material predictions to be close to uniform, making this classifier similar to a random guesser. $\mathcal{L}_{Transfer}$ is the PAISp-transfer loss, which ensures that the latent representations of the fake fingerprints are as similar as possible. λ and γ are the respective weights of the Adversarial and Transfer losses.

Results

Method	Average of all 5 sensors		
	APCER	BPCER@5	EER
MLP	**0.21**	2.23	1.90
MLPreg	0.43	**1.71**	**1.68**
CNN	4.12	12.09	7.67
CNNreg	**0.81**	**3.79**	**2.13**

- Overall, the regularization technique improves the PAD robustness of both the models (MLP and CNN).
- MLP achieved slightly better performance than the CNN, but increasing the amount of training data will certainly increase the performance of the second approach (end-to-end).

Method	Cross Match		Digital Persona		Green Bit		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 [1, 2]	1.68	≈ **0.80**	**0.60**	≈ 10.00	4.00	≈ 5.00	2.09	≈ 5.27
Park et al [3]	**0.00**	-	11.00	-	8.00	-	6.33	-

- Regularized CNN model outperformed the state of the art solutions against unseen attacks.

[1] Luca Ghiani et al. "Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015". In: Image and Vision Computing 58 (2017), pp. 110–128.
[2] Valerio Mura et al. "LivDet 2015 - Fingerprint Liveness Detection Competition 2015". In: Sept. 2015.
[3] E. Park et al. "Presentation Attack Detection Using a Tiny Fully Convolutional Network". In: IEEE Transactions on Information Forensics and Security 14.11 (2019), pp. 3016–3025.

Aknowledgements

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.

[1] INESC TEC, Porto, Portugal
[2] Faculdade de Ciências da Universidade do Porto, Porto, Portugal
[3] Faculdade de Engenharia da Universidade do Porto, Porto, Portugal