Towards Fingerprint Presentation Attack Generation using Generative Adversarial Networks

Leonardo Capozzi, Tiago Gonçalves, Jaime S. Cardoso, Ana Rebelo

Motivation

Fingerprint recognition systems have shown to be reliable in terms of accuracy, speed and purported security, but present several vulnerabilities against spoof attacks

To overcome this flaw, several automated spoofing detection models have been developed

Hypothesis

If one could **learn a distribution that contains all possible presentation attacks (PAs)**, then it should be possible to **learn a function that could correctly discriminate against *bona fide* (BF) and unseen PAs**, without the need of explicitly using them during the training phase

Contributions

Following the work proposed by Pereira et al. [1], we intend to extend the adversarial methodology and use generative adversarial networks (GANs) to 1) increase the quality of the generated PA species; and 2) increase the robustness of the PAD method against unseen attacks

Data

We used the LivDet2015 dataset, which was developed for the 2015 edition of the Liveness Detection Competition

Our data processing pipeline is employed as follows: **1) images are converted into the grey-scale format**; **2) images are then re-scaled into 110% of their original size through the addition of padding, with pixel values = 255**; **3) a centre-crop operation is then applied to assure that images keep their final size as 64 × 64 and that the fingerprint is in the centre of the image as well**; **4) the pixel values of the images are then re-scaled to be in the closed interval of [−1, 1]**

GAN and cGAN

The GAN model we use in this work is based on the class of **Deep Convolutional GANs (DCGANs) [2]**, and the **cGAN model uses the U-Net architecture for the generator [3]**

We start the training of the GAN with the generation of a latent-space vector nz of size 64 filled with random numbers sampled from a normal distribution with mean 0 and variance 1

Fingerprint Presentation Attack Detection

For the fingerprint presentation attack detection (FPAD) task, we used DenseNet121 as backbone. We added a single neuron (linear layer) with the sigmoid activation at the end of the architecture as the classifier

Regarding data augmentation, we employ three different strategies: **1) Baseline training without data augmentation (M1)**; **2) Training with synthetic images generated with the GAN model, in which we add new images (bona fide and PA) generated with the different GAN models to the train set (M2)**; **3) Training with synthetic images generated with the cGAN model, in which we add new images (PA only) generated with the cGAN models to the train set (M3)**

Results and Discussion

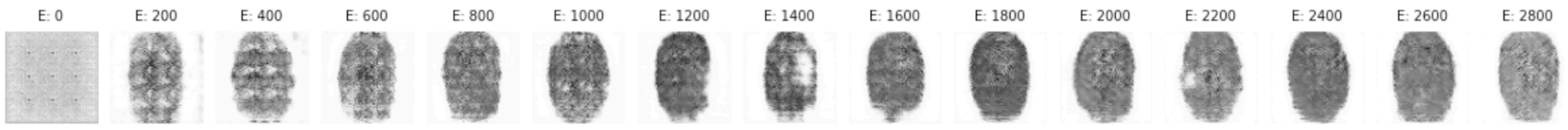

Figure 1: Examples of images generated by our GAN model per epoch (real fingerprints from the Cross Match dataset).

Table 1: Accuracy results obtained for the M1–M3 models for the different datasets and related materials. Best results highlighted in bold.

Material / Dataset	Cross Match			Digital Persona			Hi Scan		
	M1	M2	M3	M1	M2	M3	M1	M2	M3
Ecoflex	**0.9130**	0.8859	0.8232	-	-	-	-	-	-
Playdoh	**0.9568**	0.8787	0.9062	-	-	-	-	-	-
Latex	-	-	-	**0.9648**	0.9640	0.9496	**0.9752**	0.9744	0.9712
Gelatine	-	-	-	0.9024	0.9112	**0.9160**	**0.9144**	0.9008	0.9064
Wood Glue	-	-	-	0.9384	**0.9392**	0.9384	0.8600	0.8704	**0.8776**

References

[1] Joao Afonso Pereira, Ana F Sequeira, Diogo Pernes, and Jaime S Cardoso. A robust fingerprint presentation attack detection method against unseen attacks through adversarial learning. In 2020 International Conference of the Biometrics Special Interest Group (BIOSIG), pages 1–5. IEEE, 2020.

[2] Alec Radford, Luke Metz, and Soumith Chintala. Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434, 2015.

[3] Ana F Sequeira, Shejin Thavalengal, James Ferryman, Peter Corcoran, and Jaime S Cardoso. A realistic evaluation of iris presentation attack detection. In 2016 39th International Conference on Telecommunications and Signal Processing (TSP), pages 660–664. IEEE, 2016.

Acknowledgements

This work is co-financed by Component 5 - Capitalization and Business Innovation, integrated in the Resilience Dimension of the Recovery and Resilience Plan within the scope of the Recovery and Resilience Mecha- nism (MRR) of the European Union (EU), framed in the Next Generation EU, for the period 2021 - 2026, within project NewSpacePortugal, with reference 11, and by FCT – Fundação para a Ciência e a Tecnologia within the PhD grants “2020.06434.BD” and “2021.06945.BD”.