Università degli Studi
di Cagliari, Italy

Università degli Studi di
Napoli Federico II, Italy

Fingerprint Adversarial Presentation Attack in the Physical Domain

Stefano Marrone, Roberto Casula, **Giulia Orrù**,
Gian Luca Marcialis, Carlo Sansone

MMForWILD Milan, 10 | 15 January 2021

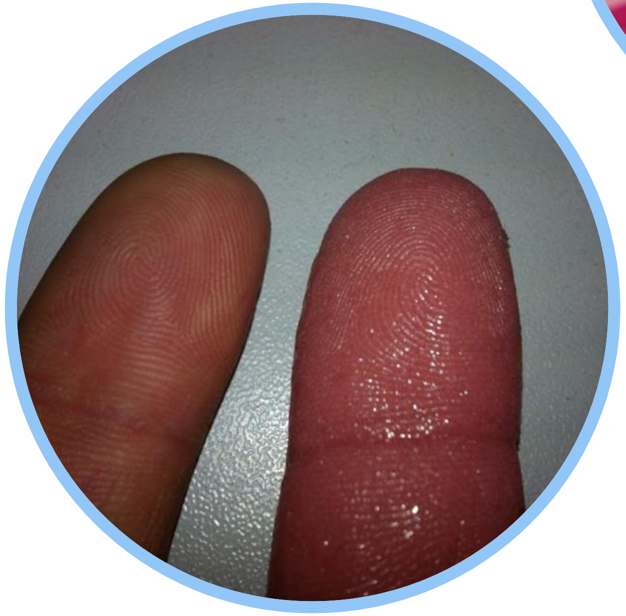
Fingerprint Presentation Attack

- Present artificial replicas of fingerprints to a sensor

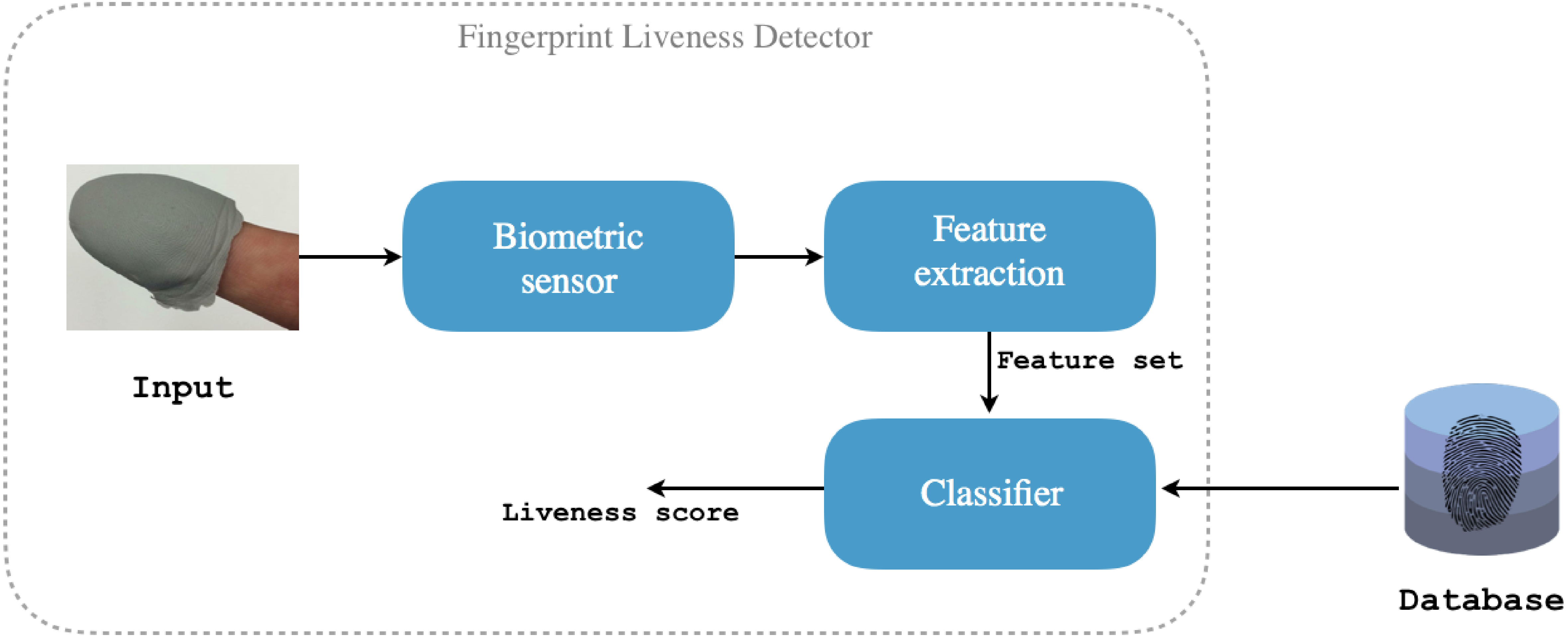
- Different materials such as silicone, gelatine, play-doh, ecoflex, 2D printed paper, 3D printed material, latex, etc.

- Consensual method: collaborative user, acquisition with cast of the finger

- Un-consensual method: acquisition from latent fingerprints

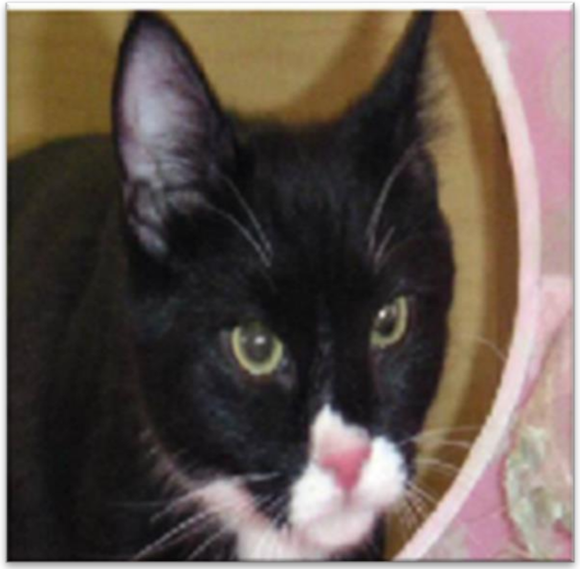


Fingerprint Presentation Attack Detection (FPAD)

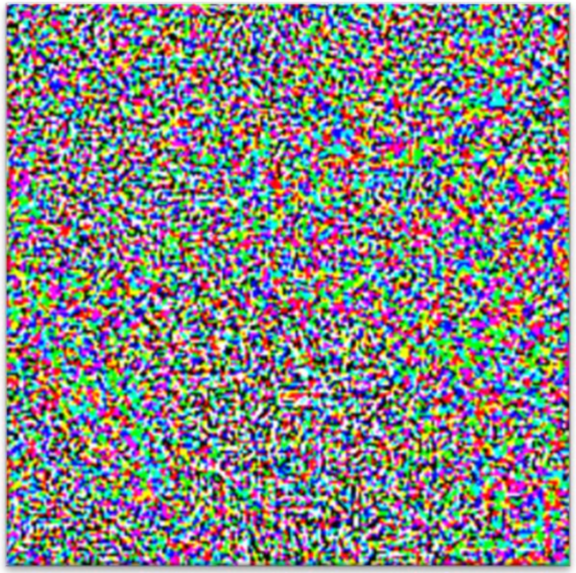


Adversarial Perturbations

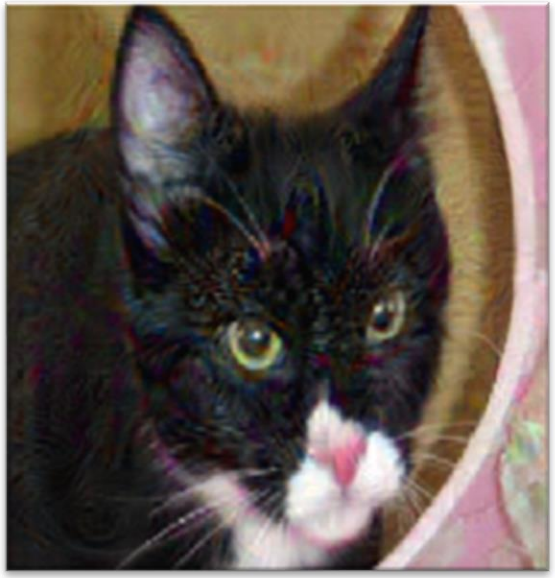
- Injection of a imperceptible noise in order to mislead a CNN



Cat (Prob. 99,2%)



Noise

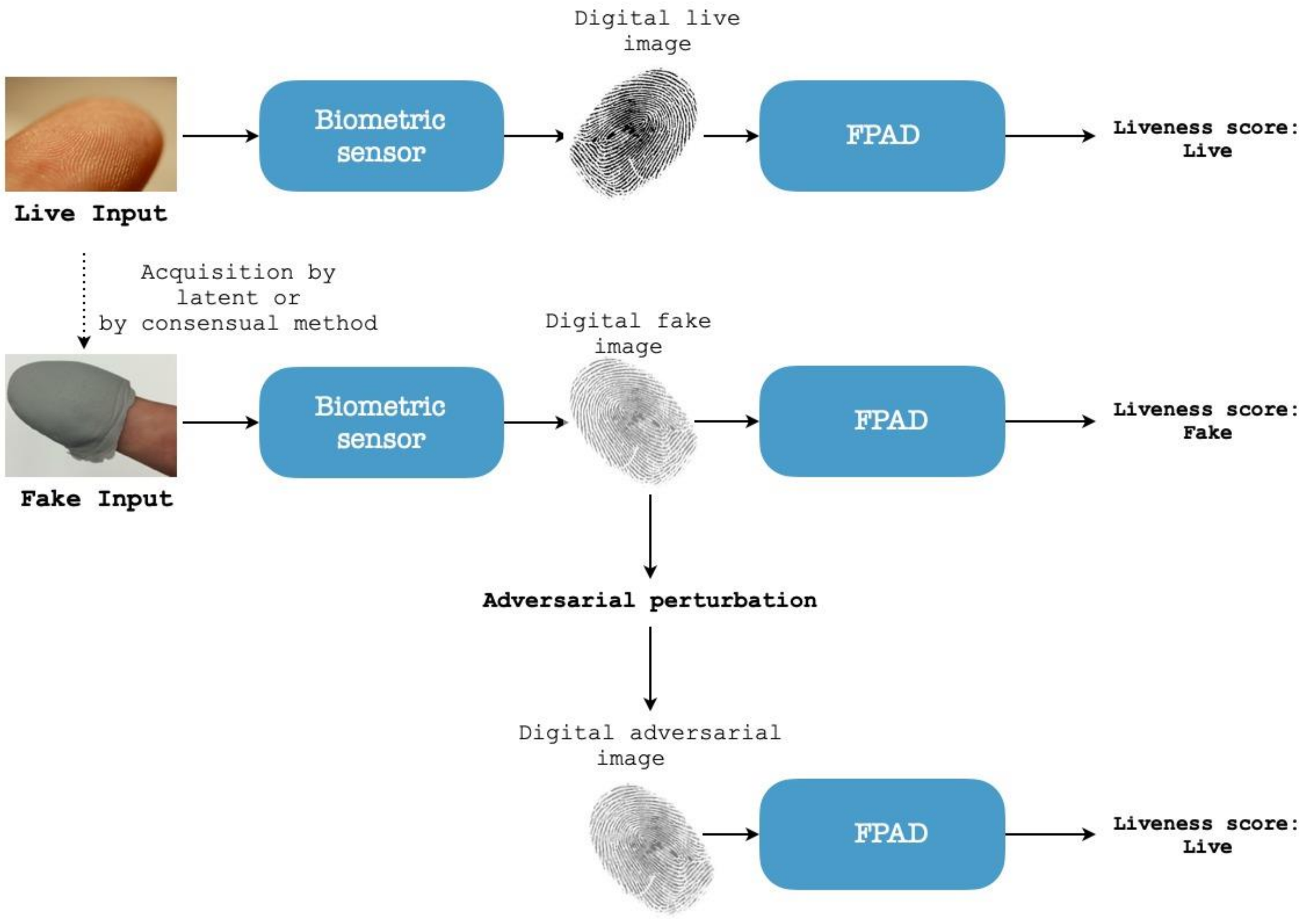


Dog (prob. 89,7%)

Szegedy et al. “Intriguing properties of neural networks”, arXiv:1312.6199 (2014)

Moosavi-Dezfooli, et al. “Deepfool: a simple and accurate method to fool deep neural networks”, in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2016)

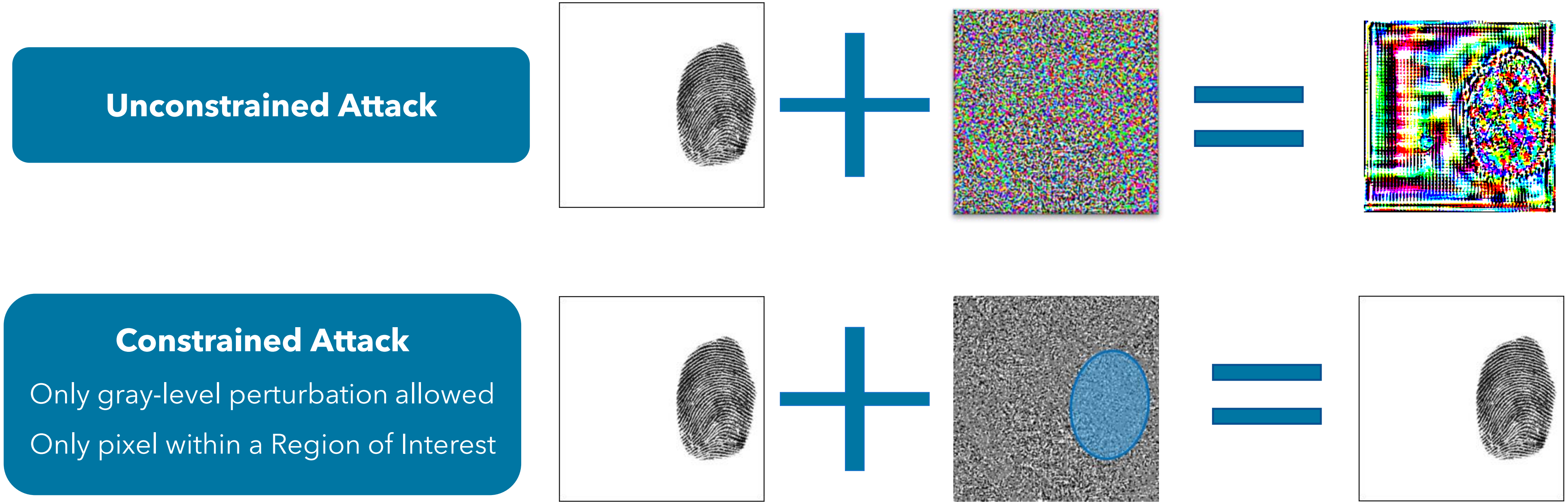
Adversarial Perturbetions for Fingerprint images



Marrone, S., Sansone, C.: Adversarial perturbations against fingerprint based au-thentication systems. IEEE International Conference on Biometrics pp. 1–6 (2019).

Adversarial Perturbetions for Fingerprint images: a constrained attack

- Fingerprints images are different from natural images and the injected noise could be very visible and difficult to hide



Unconstrained Attack

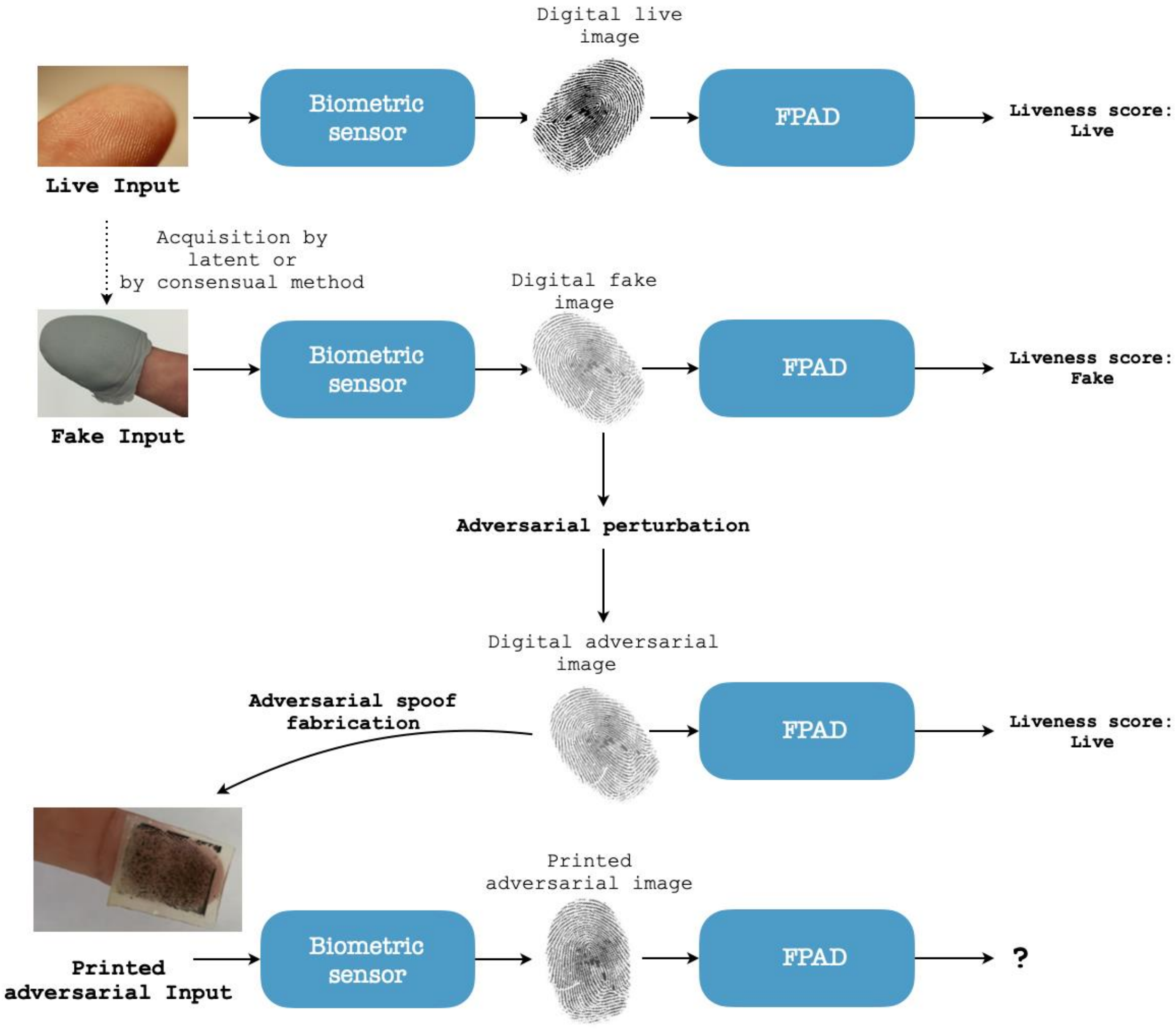
Constrained Attack

Only gray-level perturbation allowed

Only pixel within a Region of Interest

Fingerprint Adversarial Presentation Attack in the Physical Domain

- move the adversarial attacks from the digital domain to the physical one



Spoofs creation and acquisition

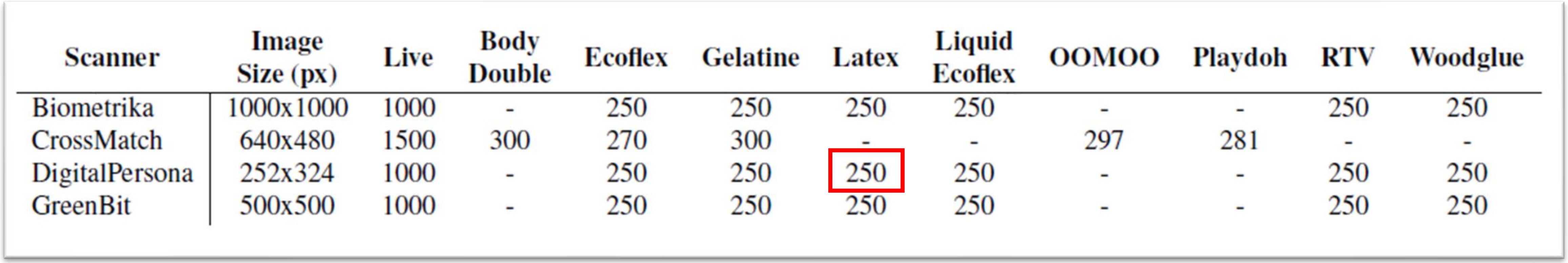
1. We create a positive mould by inverting the digital adversarial images
2. We printed several inverted fingerprints on the same sheet with a laser printer
3. A layer of latex is deposited over the prints of the individual perturbed fingerprints
4. We acquire each fake through the fingerprint sensor

Experimental Protocol

Dataset: LivDet 2015[1] -(Digital Persona – Latex)

FPAD: LivDet 2015 edition winner[2]

Adversarial perturbation algorithm: DeepFool[3]



Scanner	Image Size (px)	Live	Body Double	Ecoflex	Gelatine	Latex	Liquid Ecoflex	OOMOO	Playdoh	RTV	Woodglue
Biometrika	1000x1000	1000	-	250	250	250	250	-	-	250	250
CrossMatch	640x480	1500	300	270	300	-	-	297	281	-	-
DigitalPersona	252x324	1000	-	250	250	250	250	-	-	250	250
GreenBit	500x500	1000	-	250	250	250	250	-	-	250	250

[1] Mura, V., Ghiani, L., Marcialis, G.L., Roli, F., Yambay, D.A., Schuckers, S.A.: Livdet 2015 fingerprint liveness detection competition 2015. In: Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on.pp. 1–6. IEEE (2015)

[2] Nogueira, R.F., de Alencar Lotufo, R., Machado, R.C.: Fingerprint liveness detection using convolutional neural networks. IEEE transactions on information forensics and security, 1206–1213 (2016)

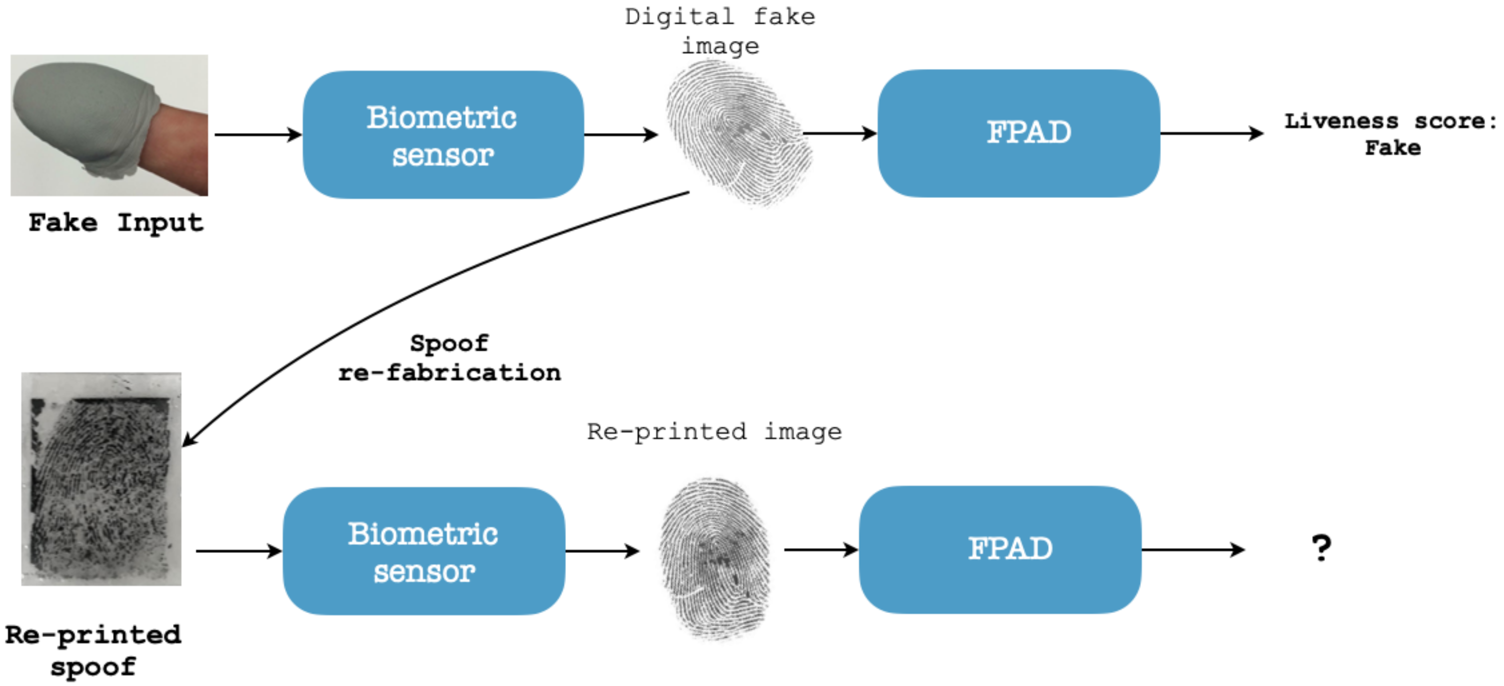
[3] Moosavi-Dezfooli, et al. "Deepfool: a simple and accurate method to fool deep neural networks", in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2016)

Experimental Protocol

- only fake fingerprint correctly classified as fake by the FPAD underwent the adversarial perturbation process (242 of 250)
- each spoof was acquired 10 with small rotations of the spoof on the sensor

Impact spoof re-fabrication

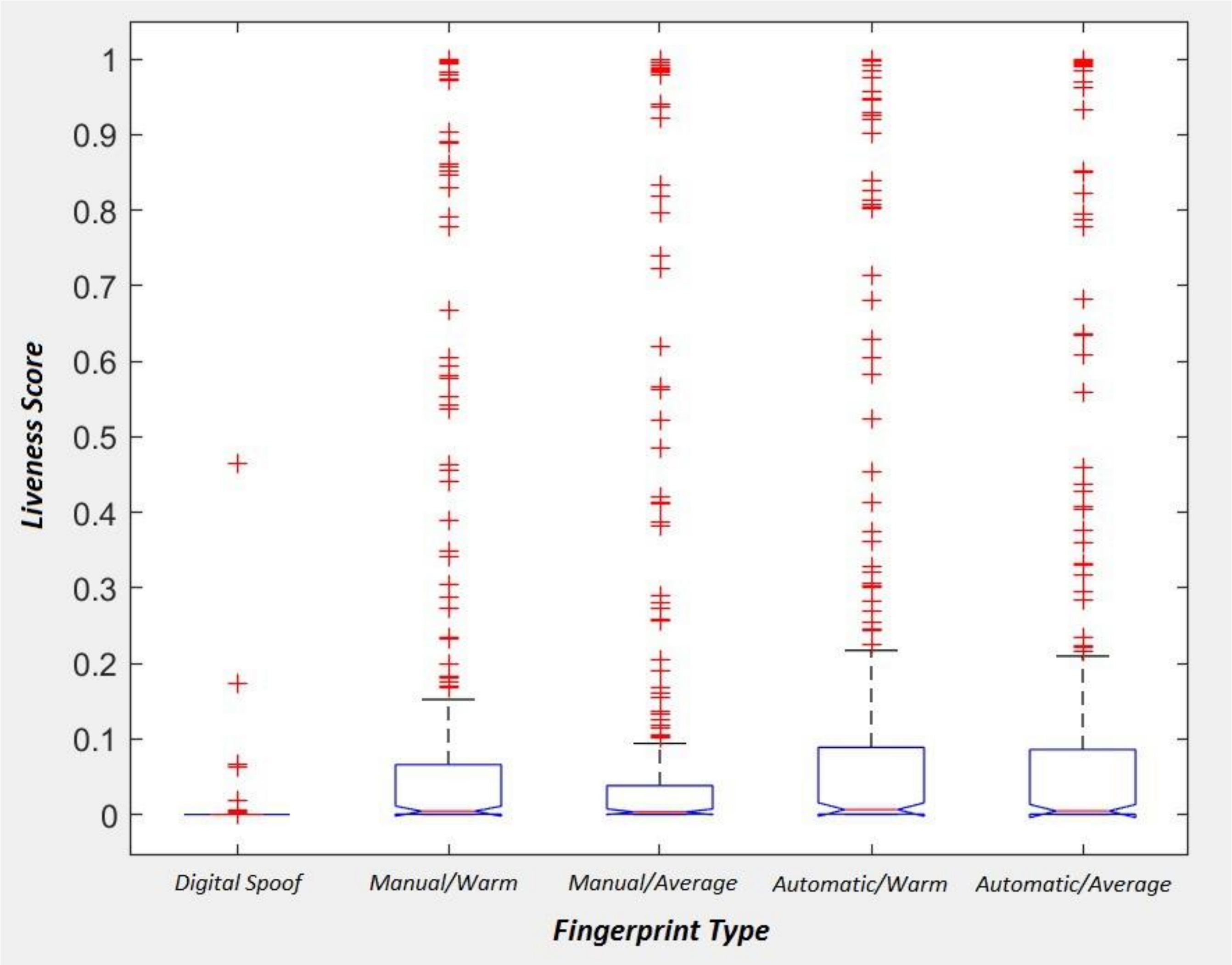
- verify how much the acquisition conditions and the pre-printing pre-processing influenced the liveness score



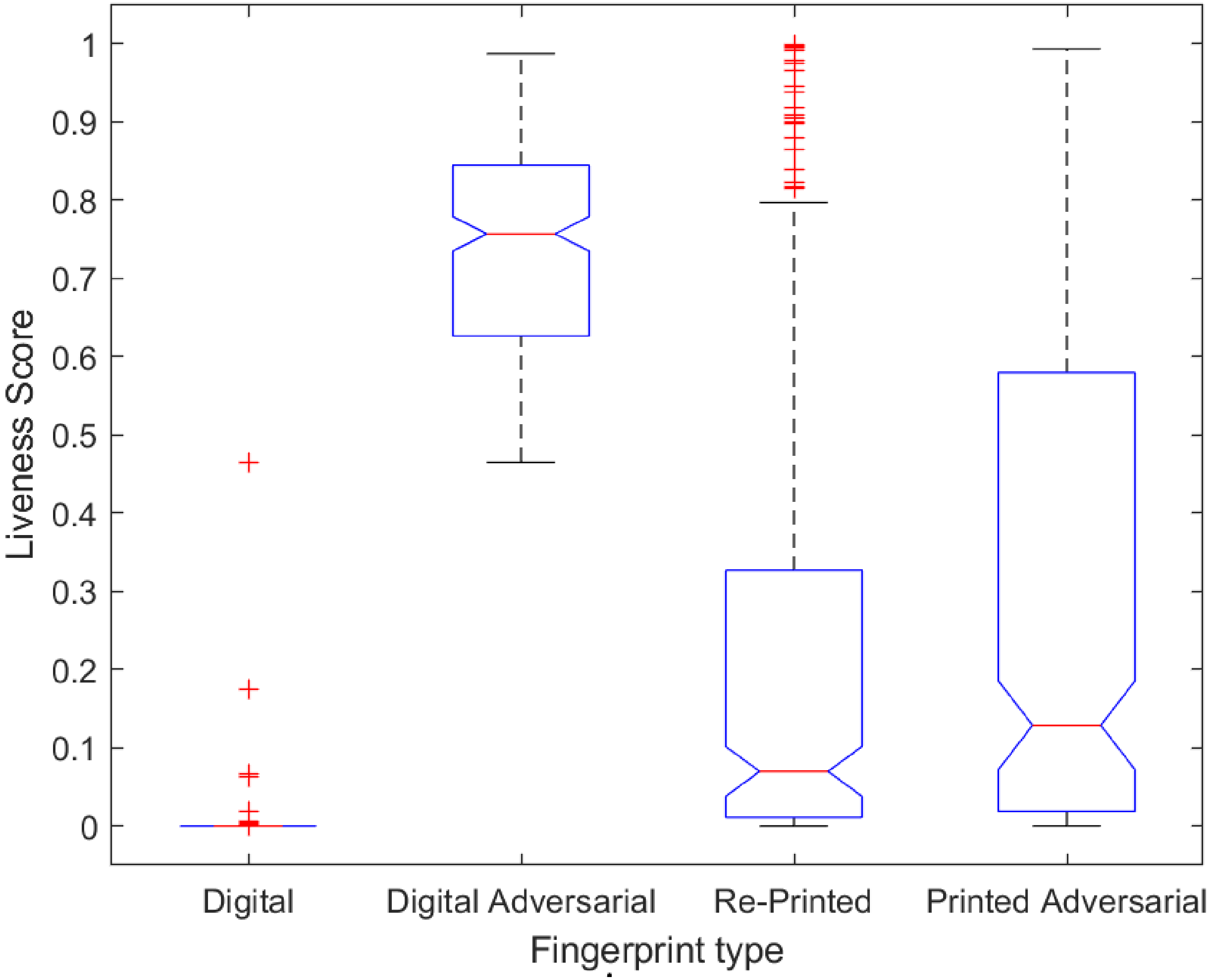
Acquisition conditions and pre-printing pre-processing influence

- Warm: T> 30° C
- Average: about T=20° C

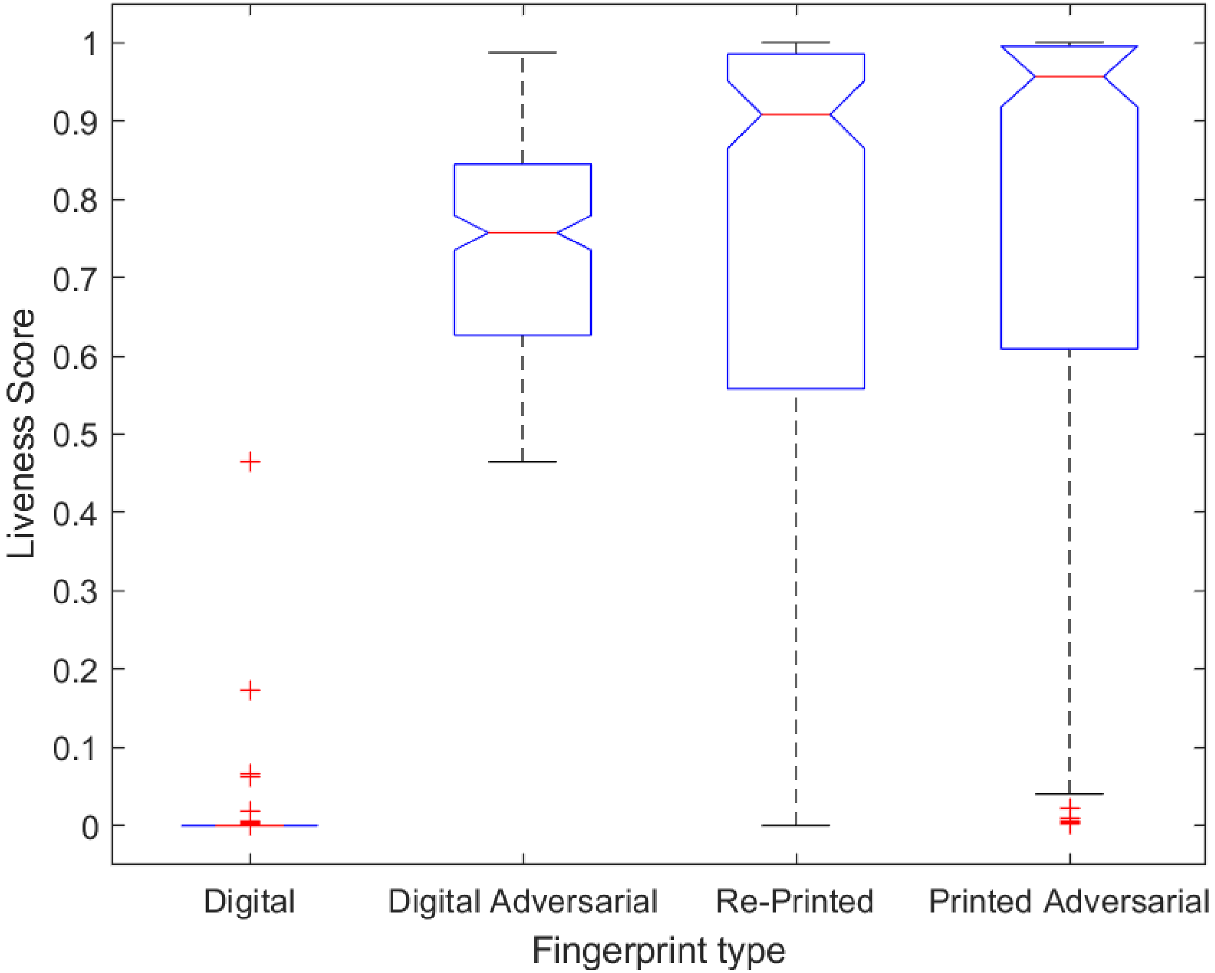
- Manual: inverting and resizing the fakes individually using an image editor
- Automatic: reversing and resizing the images via a MATLAB code



Results



Liveness Score
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Digital
Digital Adversarial
Re-Printed
Printed Adversarial
Fingerprint type



Liveness Score
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Digital
Digital Adversarial
Re-Printed
Printed Adversarial
Fingerprint type

Conclusions

- Evaluation of the threat of a physical adversarial attack against a CNN-based Fingerprint Presentation Attack Detector: feasible and dangerous
- Comparison between a physical adversarial attack with the simple re-printing of the original digital images
- Future works: black-box attack scenario and latent spoof fingerprints

Thanks for your attention! Questions?

giulia.orru@unica.it