Fingerprint Adversarial Presentation Attack in the Physical Domain

Stefano Marrone
University of Naples Federico II
Via Claudio 21, 80125, Naples (Italy)
Email: stefano.marrone@unina.it

Roberto Casula
University of Cagliari
Piazza d'Armi, 09123 Cagliari (Italy)
Email: roberto.casula@unica.it

Giulia Orrù
University of Cagliari
Piazza d'Armi, 09123 Cagliari (Italy)
Email: giulia.orru@unica.it

Gian Luca Marcialis
University of Cagliari
Piazza d'Armi, 09123 Cagliari (Italy)
Email: marcialis@unica.it

Carlo Sansone
University of Naples Federico II
Via Claudio 21, 80125, Naples (Italy)
Email: carlo.sansone@unina.it

***Abstract*—With the advent of the deep learning era, Fingerprint-based Authentication Systems (FAS) equipped with Fingerprint Presentation Attack Detection (FPAD) modules managed to avoid attacks on the sensor through artificial replicas of fingerprints. Previous works highlighted the vulnerability of FPADs to digital adversarial attacks. However, in a realistic scenario, the attackers may not have the possibility to directly feed a digitally perturbed image to the deep learning based FPAD, since the channel between the sensor and the FPAD is usually protected. In this paper we thus investigate the threat level associated with adversarial attacks against FPADs in the physical domain. By materially realising fakes from the adversarial images we were able to insert them into the system directly from the "exposed" part, the sensor. To the best of our knowledge, this represents the first proof-of-concept of a fingerprint adversarial presentation attack. We evaluated how much liveness score changed by feeding the system with the attacks using digital and printed adversarial images. To measure what portion of this increase is due to the printing itself, we also re-printed the original spoof images, without injecting any perturbation. Experiments conducted on the LivDet 2015 dataset demonstrate that the printed adversarial images achieve $\sim 100\%$ attack success rate against an FPAD if the attacker has the ability to make multiple attacks on the sensor (10) and a fairly good result ($\sim 28\%$) in a one-shot scenario. Despite this work must be considered as a proof-of-concept, it constitutes a promising pioneering attempt confirming that an adversarial presentation attack is feasible and dangerous.**

I. Introduction

Personal authentication systems based on biometrics and, in particular, on fingerprints are widespread in public security systems and personal devices, thanks to their precision and user-friendliness. Spoofing attacks, i.e. attacks to the sensor through artificial reproductions of fingerprints, have always represented a serious security threat to Fingerprint Authentication Systems (FAS) [1]. In recent years, numerous Fingerprint Liveness Detection (FLD) systems, also known as Fingerprint Presentation Attack Detection (FPAD) systems, have been proposed to counteract these attacks.

The rapid diffusion of deep-learning-based and, in particular, of Convolutional Neural Networks (CNN) based methods has made it possible to reach liveness-detection rates above 95% [2]. However, in 2013 it has been demonstrated that neural networks suffer from some new vulnerabilities [3]. This attack (known as adversarial perturbation) not only can be perpetrated at training time (known as poisoning) but also at test time (known as evasion) [4].

Adversarial perturbations are thus potentially very dangerous since an attacker could intentionally add small perturbations to an image, keeping it visually unchanged, to force the classifier's decision. On this line, some recent works already demonstrated the effectiveness of a digital attack on a CNN FPAD [5], [6]. This type of attack assumes the attackers to be able to enter the communication channel between the sensor and the neural network, making them able to submit the adversarial images as input to the FPAD. This type of attack is therefore infeasible if the system uses secure channels protected by time-stamps, physical isolation or challenge-response mechanisms [7].

Based on these considerations, we wondered if an attacker, with high knowledge of the system, could exploit adversarial perturbations to increase the possibility that their spoofs deceive a CNN-based FPADs. In other words, *the aim of this work is to analyse whether the small perturbations that modify FPAD's decision can be "printed" and exploited in an artificial and material replica of the fingerprint.*

The rest of the paper is organised as follows. Section 2 provides a brief introduction to CNN-based anti-spoofing and existing perturbation attacks. Section 3 describes the proposed attack. Section 4 evaluates the threat level of the printed adversarial images on a state-of-art fingerprint liveness detector.Section 4 draws some conclusions.

II. CNN-based FPAD and Adversarial Perturbations

Presentation attack, namely the action of "presenting" a fake fingerprint replica to a fingerprint scanner, is a common attack against Fingerprint-based Authentication Systems (FAS). Possible protection against such attacks includes the use of

Scanner	Image Size (px)	Live	Body Double	Ecoflex	Gelatine	Latex	Liquid Ecoflex	OOMOO	Playdoh	RTV	Woodglue
Biometrika	1000×1000	1000	-	250	250	250	250	-	-	250	250
CrossMatch	640×480	1500	300	270	300	-	-	297	281	-	-
DigitalPersona	252×324	1000	-	250	250	250	250	-	-	250	250
GreenBit	500×500	1000	-	250	250	250	250	-	-	250	250

TABLE I
LIVDET2015 DATASET CHARACTERISTICS. FOR EACH SCANNER, THE ACQUIRED FINGERPRINT SIZE, AND THE NUMBER OF LIVE AND FAKE FINGERPRINTS (FOR EACH SPOOFING MATERIALS) IMAGES ARE REPORTED. THE HYPHEN IN A CELL INDICATES THAT THE CORRESPONDING MATERIAL HAS NOT BEEN USED TO GENERATE FAKE FINGERPRINTS FOR THE CORRESPONDING SCANNER.

a Fingerprint Presentation Attack Detection (FPAD) module to discriminate between "live" and "fake" fingerprints. The use of an FPAD module has become more and more common since its use causes the attacker to first bypass the FPAD, by modifying a fake replica such that it is recognised as a real fingerprint.

FPAD algorithms relies on the extraction of anatomical, physiological or texture-based features from fingerprint images. Over the years, FPAD methods have been refined and recently Convolutional Neural Networks (CNNs) have been leveraged, using either the full image [8], [9] or patching it [10], allowing to reach very high accuracy levels [2].

In 2013, when CNNs had not yet spread to many applications of pattern recognition, Szegedy et al. [11], [3] demonstrated the existence of adversarial attacks against deep learning methods (including CNN), i.e. the injection of a suitable, hardly perceptible, perturbation which leads to a misclassification of the input image. This severe vulnerability has made the robustness of CNN models to adversarial attacks a key feature in modern systems. Indeed, in the last decade, adversarial attacks as the Fast Gradient SignMethod (FGSM) [12], the Basic Iterative Method (BIM) [13] and many others[3], have become more numerous, more effective and easy to perform, thanks to the availability of free and open-source toolboxes [14], [15].

This problem is particularly critic in security-related domains leveraging CNNs in one of their stages. Focusing on the case of fingerprints, the vulnerability of FPAD systems to adversarial perturbations has already been demonstrated [5], [6], describing methods designed to generate perturbed fingerprint images able to mislead a target FPAD in the digital domain. In both cases, the attacks assume that the attacker can feed the perturbed digital image directly into the CNN. Despite sufficient for a proof-of-concept, these attacks have limited applicability since most modern systems are protected from this possibility, with the attacker only having access to the sensor.

Recently, the effectiveness of an adversarial physical domain attack against a CNN-based face authentication system equipped with an anti-spoofing module has been demonstrated [16]. Printed and replay facial attacks are easy to obtain, and the authors have shown that the "fabrication" of these replicas allows for the retention of the added adversarial information.

In this manuscript we investigate whether the more complex creation of an artificial fingerprint replica allows an adversarial attack on a fingerprint presentation attack detection system in the physical domain.

III. Proposed Approach

To perform an adversarial presentation attack in the physical domain, we must identify i) a fingerprint dataset, ii) a presentation attack detector, iii) an adversarial perturbation procedure for fingerprints and iv) a way to physically realise the crafted adversarial fake replica. Following section analyse each of these points, highlighting means and choices made.

A. Fingerprints Liveness Dataset

The need for a common experimental protocol for liveness detection tasks gave rise to the gathering of fingerprints datasets. Among all those available, in this work we consider the one provided with the LivDet 2015 competition [17]. This choice is mostly driven by the availability of well-defined training and test datasets and by the availability of open-source top-performer liveness detectors trained on it. Table I briefly reports the main characteristics of the LivDet 2015 dataset.

B. Adversarial Perturbations for Fingerprints

Usually, an *adversarial perturbation* is a noise $r \in R^{(w,h,3)}$ (with w and h the width and height of a target image) crafted with the aim of misleading a target image classifier. In the context of fingerprints, an attacker not only must craft the perturbation to be as subtle (i.e. invisible) as possible but also must take into account the fact that fingerprints and natural images are visually different. Accordingly, in a previous work [5] we modified some well-known adversarial perturbation algorithms i) to inject a grey-level (i.e., the same for all the channels in the case of RGB acquisitions) noise $r \in [0, 255]$ and ii) to apply it only to the Region of Interest (ROI) delimiting the actual fingerprint. These constraints result in a perturbation that, although able to mislead an FPAD, is still imperceptible for a human operator (Figure 1). In out previous work [5] we modified three adversarial perturbation algorithms. In this work we focus only on DeepFool [18] as it showed to be the most convenient in terms of attack success rate vs required computational effort.

C. Spoof's Creation and Acquisition

The perturbation of the fingerprints through the previously described method is followed by the creation of the moulds of the adversarially perturbed images. To this aim, the fingerprints are first printed (by using a normal laser printer)

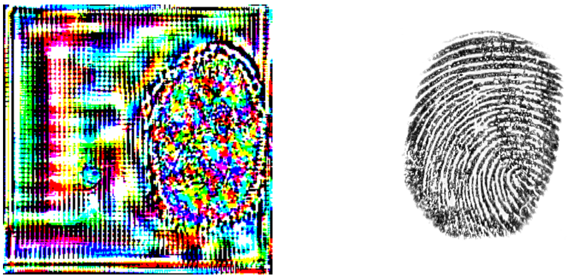

Fig. 1. Example of an unconstrained (left) and of a constrained (right) fingerprint adversarial perturbation [5].

on a transparent sheet. The fingerprints are directly printed in their real size, without the need for any resize operation (since the perturbation has been applied on their digitalised version). Instead, since the final fingerprints need to be a perfect replica of the original finger (i.e. a positive mould), the printed fingerprint must be "inverted". Finally, since the size of a fingerprint is very little when compared with a standard A4 page, we printed several fingerprints on the same sheet .

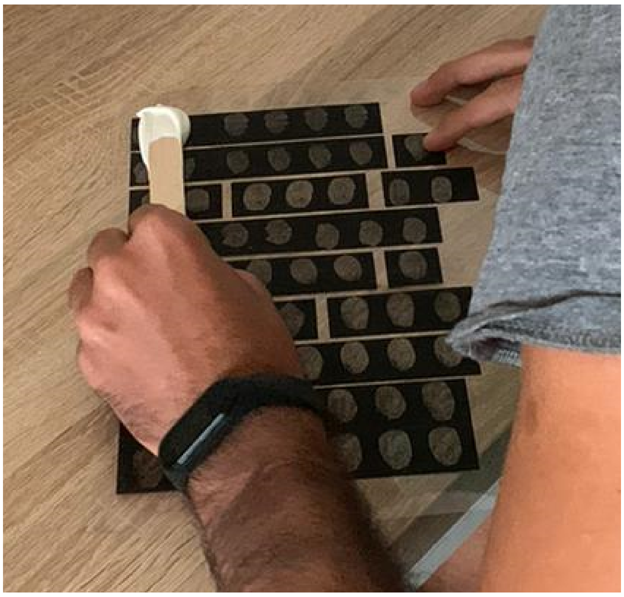

Fig. 2. Particular of the adversarial fingerprint physical spoof realisation. In the image, the expert is depositing a later of latex over the printed adversarial fingerprints. Please note that, on the same sheet, there are several fingerprints (possibly from different subjects), all inverted in the colours.

Once the sheet has been created, a layer of latex is deposited over the prints of the individual perturbed fingerprints, making sure that there is no swelling of air and that the resulting layer has an adequate thickness that allows correct removal and subsequent acquisition through the sensor (Figure 2). Indeed, if the fake is of excessively thin thickness, the removal operation from the sheet would compromise the fingerprint, resulting in a non-optimal acquisition. The resulting fingerprint (Figure 3 is then posed over the scanner to perform the actual adversarial presentation attack.

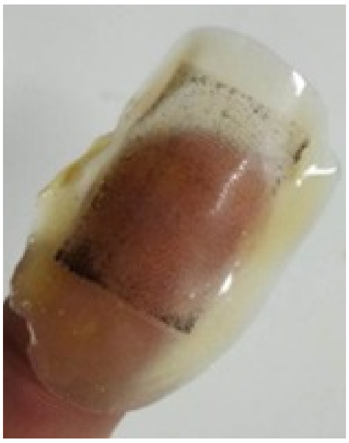

Fig. 3. A physical adversarial fake fingerprint obtained using the method described in this paper.

D. Attacking the CNN for Liveness Detection

Over the years, LivDet competitors moved from "classical" computer vision algorithms to solution leveraging Deep Convolutional Neural Networks (CNNs). Indeed, the LivDet 2015 edition winner [8] demonstrated that also FPAD can benefit from CNNs, being able to reach accuracy levels and intra-materials and intra-sensors generalisation ability never reached until that moment. In particular, the authors made use of a VGG19 network [19], pre-trained on ImageNet and fine-tuned to recognise live from spoof fingerprints. To improve the network generalisation ability, the authors augmented the dataset by extracting five patches from each fingerprint, obtaining a final dataset 10 times bigger than the original one. Finally, to match the VGG19 input layer expected image dimensions, each patch is resized to 224×224 pixels.

In our previous work [5] we attacked the aforementioned Vgg16-based FPAD showing how to effectively bypass it by means of adversarial perturbations. In that case, all the experiments were performed in the digital domain. Indeed, although the attack was already designed to be "printed" for real-world application, the actual fake replica crafting and its use for a real presentation attack has never been performed.

In this paper we want to fill the gap by proposing a proof-of-concept for an adversarial presentation attack. In particular, we analyse whether it is possible to realise a tangible replica of an adversarial fingerprint that is still able to bypass the liveness detector. To this aim, we design the following attack scenario (Figure 4):

- We sample a set of subjects and acquire their fingerprints to be submitted to the FPAD in order to calculate the liveness score (first row in figure 4);
- For all the enrolled subjects we also consensually acquire a mould for each fingerprint. These will be then used to craft fake fingerprint replicas to be submitted to the FPAD to calculate the liveness score (second row in figure 4);
- We leverage the adversarial fingerprint generation procedure [5] to determine, for each fake fingerprint crafted in

the previous stage, the noise to add needed to mislead the FPAD. The resulting adversarial fake fingerprints are then submitted to the FPAD in order to calculate the liveness score (third row in figure 4);

- Finally, for each adversarial fake fingerprint, we craft a physical replica to be submitted, present it to the scanner and submit the acquisition to the FPAD in order to calculate the liveness score (fourth row in figure 4).

To evaluate the attack success rate, we consider only *fake* fingerprints form the official LivDet2015 test dataset (since an attacker is usually interested only in making fake replicas recognised as live). As this work aims to provide a proof of concept, we tried to limit the influence of as many aspects as possible. Therefore, among all the scanners and materials, we only focus on Digital Persona as scanner, Latex as spoofing material, the official LivDet2015 winner [8] as FPAD and DeepFool [18] (modified to work with fingerprints as in [5]) as adversarial perturbation algorithm.

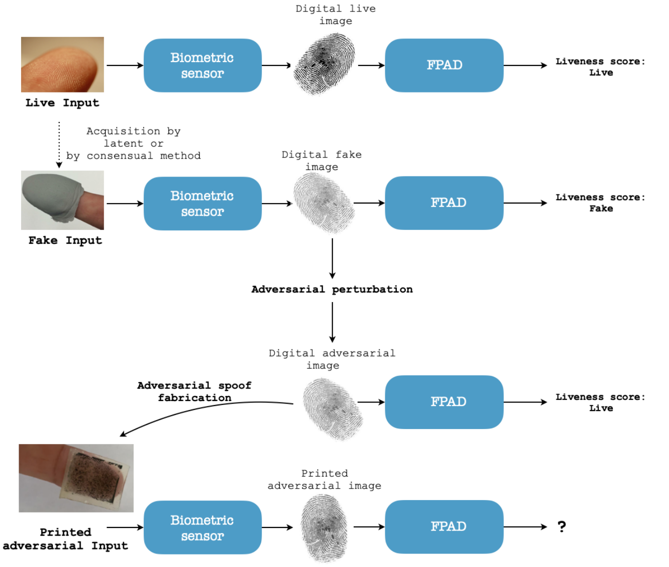

Fig. 4. Adversarial presentation attack schema. In the first row, the subject fingerprint is acquired; in the second row, a consensual fake replica is crafted; in the third row the (digital) adversarial fingerprint is crafted; finally, in the fourth row, the adversarial replica is printed and acquired. In all the stage, the target FPAD is used to evaluate the liveness score of the corresponding stage fingerprints.

Although all the stages are intended to try to minimise the impact of any external factor, the physical fingerprint crafting procedure might itself introduce a bias in the liveness score. Therefore, for all the fake fingerprints (stage two of the previous schema) we also crafted the corresponding physical replica without any adversarial perturbation applied (Figure 5), with the aim of measuring the effect that a simple print and re-acquisition has on the liveness score.

IV. Results

In this section, we evaluate the actual threat of the proposed adversarial attack in the physical domain.

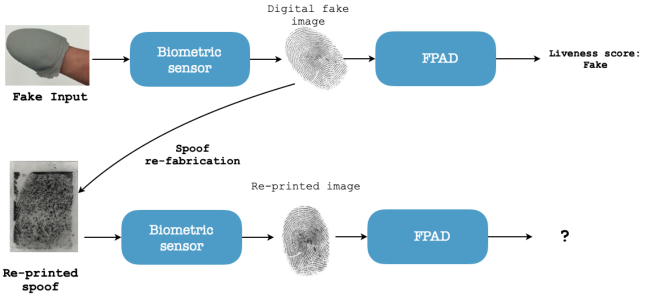

Fig. 5. Schema for the evaluation of the impact that spoof re-fabrication from the digital image has on the FPAD score.

The first evaluation served to verify how much the acquisition conditions and the pre-printing pre-processing influenced the liveness score. In this preliminary experiment, each spoof was acquired once. The Figure 6 shows the comparison between manual and automatic pre-processing and between acquisitions in a warm environment (30° Celsius) and an environment with average temperatures (about 20° Celsius).

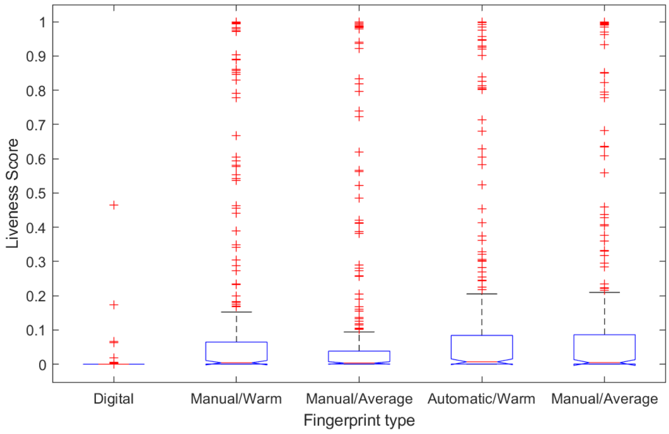

Fig. 6. Boxplot of the liveness scores of the 250 latex re-printed samples crafted with different acquisition and pre-processing methods: the manual method, which consists in inverting and resizing the fakes individually using an image editor and printing the paginated fingerprints; the automatic procedure, reversing and resizing the images via a MATLAB code. The difference between Warm and Average depends on the temperature in the room during printing and re-acquisition: 30° Celsius for Warm and about 20° Celsius for Average.

The boxplots show that the different acquisitions conditions and pre-processing methods do not particularly affect liveness results. However, it is important to note that through the sole re-fabrication of the fingerprint from its digital spoof replica, most of the scores ($\sim$ 80% for all the cases reported in the boxplots) incur in an increase of the liveness score, with a portion ($\sim$ 12%) of the re-printed fingerprint able to mislead the FPAD.

Since, as aforementioned, the fake realisation procedure does not really affect the liveness score, all the following experiments were performed by printing the fingerprint using the automatic method and average temperature. It is also worth to note that, for a fair result analysis, only fake fingerprint correctly classified as fake by the FPAD underwent the adversarial perturbation process (242 of 250). Moreover, each spoof was acquired 10 times (for a total of 2420 acquisitions) with small rotations of the spoof on the sensor. This rotation is done to verify the efficacy of the detector by providing the same fingerprint but in slightly different conditions and therefore focusing on different patches of the image. To simplify the notation, we also introduce the following terms: *Digital*, referring to the digital version of a clean (i.e. non perturbed) spoof fingerprint; *Re-Print*, referring to the printed and re-acquired version of a clean spoof fingerprint; *Digital Adversarial*, referring to the digital version of an adversarially perturbed fingerprint; *Printed Adversarial*, referring to the printed and acquired version of an adversarially perturbed fingerprint (i.e. the actual adversarial presentation attack).

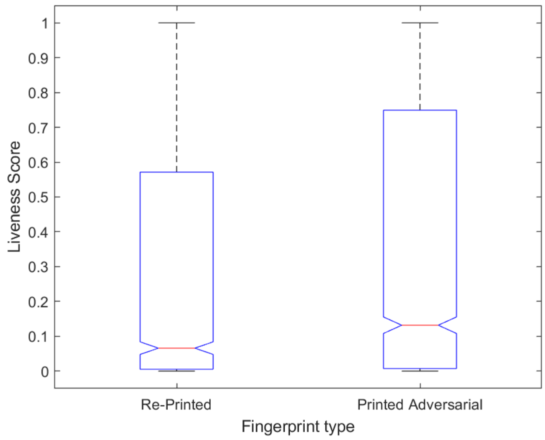

Fig. 7. Comparison of the liveness scores for the re-printed spoofs and for the printed adversarial replicas.

In Figure 7 the comparison of the liveness scores for the printed adversarial spoofs and for the re-printed spoofs is reported in order to highlight how much the improvement in the score is due to the addition of the perturbation. Although the median scores (red lines in the boxplots) are smaller than 0.5 (i.e. classified as fake), a high percentage of Printed Adversarial spoofs (specifically 32.77% against the 27.81% of the Re-Printed spoofs case) deceive the target FPAD. Part of the increase in scores is given by the re-printing process but the perturbations inserted in the images determine a further increase.

To properly assess the danger of the attack it is necessary to compare these scores with the original scores. Figure 8 shows the comparison between original scores, digital adversarial attack, re-print, and printed adversarial attack. For the last two, we plotted the median values (upper plot) and the maximum values (bottom plot) of the scores on the 10 acquisitions. From the comparison between originals and digital adversarial, we see that the images initially classified as fake, after the perturbations are classified as live in the 99.59% of the cases. On the other hand, the comparison between the median value and the maximum value of the scores of the attacks printed on the 10 acquisitions suggests some important evidence: i) the scores vary considerably based on the position of the spoof on the sensor; ii) the perturbation is not lost during the printing process but it could be lost during the submission of the spoof on the sensor; iii) an attacker can manage to bypass a target FPAD in 10 presentations of the printed adversarial spoof. What is surprising to find is the fact that even with the sole reprint of the digital spoof image it might be possible to mislead a CNN-based classification. In particular, focusing on the plot of the maximum value, 77.27% of the attacks with the re-print strategy and 80.17% with the adversarial printed are successful. This result is achievable with unrestricted (or limited to up to 10 trials) access to the sensor (multiple attacks with the same spoof). If we bring ourselves to more stringent conditions, where the attacker has only one chance of attack (simulated with the median of the scores on the 10 acquisitions) the success rates drop significantly, going down to 20.25% for the re-printed attack and to 28.51% for the adversarial printed attack.

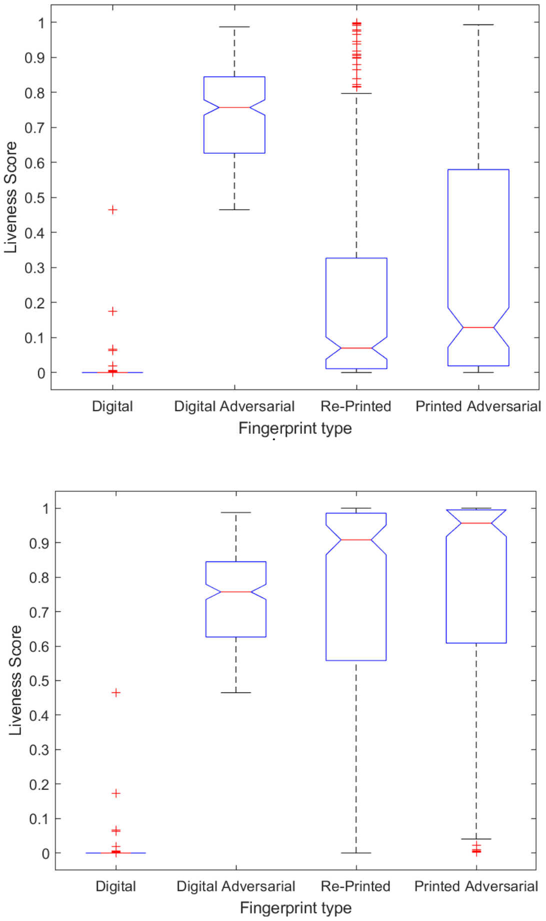

Fig. 8. Comparison between original scores *Digital*, *Digital Adversarial* attack, *Re-Print*, and *Printed Adversarial* attacks. For the last two we plotted the median values (upper plot) and the maximum values (bottom plot) of the scores obtained by the 10 acquisitions.

Results show that, although more effective than the sole re-print, the adversarial perturbed images suffer from the printing procedure, highlighting the need for a more print-resilient adversarial procedure and/or for a more adversarial-aware printing procedure. Nonetheless, these attacks pose a serious threat to CNN-based FPADs that usually report accuracy $> 90\%$ on most of the available fingerprint datasets.

V. Conclusions

In this work, we evaluated the threat of a physical adversarial attack against a CNN-based Fingerprint Presentation Attack Detector (FPAD). Crafting materially an adversarial fingerprint (i.e. a spoof fingerprint modified by means of a fingerprint adversarial perturbation algorithm) we have shown that it is possible to move these attacks from the digital domain to the physical one. This makes adversarial perturbations more dangerous, as they can be performed by an attacker having only access to the sensor. We compared this physical adversarial attack with the simple re-printing of the original digital images to assess how much the latter influenced the liveness score.

The experimental results obtained on the LivDet 2015 dataset, using the winning CNN of the same edition as FPAD [8] and a modification of the DeepFool [18], [5] as adversarial attack, showed the feasibility and danger of these printed attacks. Surprisingly, the only re-printing of the original spoofs led to an increase in liveness scores, constituting a low effort attack. The reduced difference ($\sim 3\%$) between the increase in score obtained through simple re-printing and the adversarial printed image show that although the perturbations remain and affect the liveness score even after printing, the biggest portion of it is destroied by the printing procedure. This is further confimed by the fact that the full-digital attack obtains an almost 100% success rate. Therefore, despite this work constitutes a promising pioneering attempt confirming that an adversarial presentation attack is feasible and dangerous, a more in-depth study is necessary to render the procedure more robust and effective.

A shred of important evidence is that the position of the fake on the sensor greatly influences the result. As experimental evidence, it turned out that with a maximum of 10 acquisitions it is possible for the attacker to cheat the FPAD system. This work is limited to a single FPAD and a single perturbation method. It will be thus important to evaluate how other CNN-based FPADs classify printed adversarial fingerprints. Furthermore, it will be important to evaluate whether the matching information is altered by the perturbation or by the printing process. These aspects, as well as the use of black-box attack scenario and of latent spoof fingerprints, will be faces in futures works.

References

[1] S. Marcel, M. S. Nixon, J. Fiérrez, and N. W. D. Evans, Eds., *Handbook of Biometric Anti-Spoofing - Presentation Attack Detection, Second Edition*, ser. Advances in Computer Vision and Pattern Recognition. Springer, 2019. [Online]. Available: https://doi.org/10.1007/978-3-319-92627-8

[2] G. Orrù, R. Casula, P. Tuveri, C. Bazzoni, G. Dessalvi, M. Micheletto, L. Ghiani, and G. L. Marcialis, "Livdet in action - fingerprint liveness detection competition 2019," in *2019 International Conference on Biometrics (ICB)*, 2019, pp. 1–6.

[3] N. Akhtar and A. Mian, "Threat of adversarial attacks on deep learning in computer vision: A survey," *IEEE Access*, vol. 6, pp. 14 410–14 430, 2018.

[4] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognition*, vol. 84, pp. 317 – 331, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320318302565

[5] S. Marrone and C. Sansone, "Adversarial perturbations against fingerprint based authentication systems," *IEEE International Conference on Biometrics*, pp. 1–6, 2019.

[6] J. Fei, Z. Xia, Y. Peipeng, and F. Xiao, "Adversarial attacks on fingerprint liveness detection," *EURASIP Journal on Image and Video Processing*, vol. 2020, 12 2020.

[7] B. Biggio, G. Fumera, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition : A review on biometric system security from the adversarial machine-learning perspective," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 31–41, 2015.

[8] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE transactions on information forensics and security*, vol. 11, no. 6, pp. 1206–1213, 2016.

[9] H.-U. Jang, H.-Y. Choi, D. Kim, J. Son, and H.-K. Lee, "Fingerprint spoof detection using contrast enhancement and convolutional neural networks," in *Information Science and Applications 2017*, K. Kim and N. Joukov, Eds. Singapore: Springer Singapore, 2017, pp. 331–338.

[10] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2190–2202, 2018.

[11] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, "Intriguing properties of neural networks," *arXiv preprint arXiv:1312.6199*, 2013.

[12] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2015.

[13] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," *arXiv preprint arXiv:1607.02533*, 2017.

[14] M.-I. Nicolae, M. Sinn, M. N. Tran, B. Buesser, A. Rawat, M. Wistuba, V. Zantedeschi, N. Baracaldo, B. Chen, H. Ludwig *et al.*, "Adversarial robustness toolbox v1. 0.0," *arXiv preprint arXiv:1807.01069*, 2018.

[15] J. Rauber, R. Zimmermann, M. Bethge, and W. Brendel, "Foolbox native: Fast adversarial attacks to benchmark the robustness of machine learning models in pytorch, tensorflow, and jax," *Journal of Open Source Software*, vol. 5, no. 53, p. 2607, 2020.

[16] B. Zhang, B. Tondi, and M. Barni, "Adversarial examples for replay attacks against cnn-based face recognition with anti-spoofing capability," *Computer Vision and Image Understanding*, vol. 197-198, p. 102988, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1077314220300606

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

[18] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: a simple and accurate method to fool deep neural networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2016, pp. 2574–2582.

[19] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.