Digitally synthetized fingerprint spoofs: a threat for anti-spoofing systems?

Abdarahmane Wone, Joël di Manno, Christophe Rosenberger, Christophe Charrier

DIGITALLY SYNTHETIZED FINGERPRINT SPOOFS: A THREAT FOR ANTI-SPOOFING SYSTEMS ?

Abdarahmane WONE*†, Joël DI MANNO*, Christophe ROSENBERGER† and Christophe CHARRIER†
*FIME EMEA, 14000 Caen, France
abdarahmane.wone@unicaen.fr, joel.dimanno@fime.com
†Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
christophe.rosenberger@ensicaen.fr, christophe.charrier@unicaen.fr

***Abstract*—Ensuring security on biometric systems has always been a high priority concern. Certification of biometric systems involves the testing of the system's performance and its resistance to spoof attacks. The anti-spoofing test implies the creation and scan of multiples physical spoofs. This requests laboratory expertise and high amount of time for spoofs creation. In this paper, we propose a new solution based on deep learning to translate genuine fingerprint images and transform them into what they would look like if they were created from known spoof materials usually involved in fingerprint spoofing tests. Digitally Synthetized Fingerprint Spoofs (DSFS) help to cover a larger number of spoofs materials than it would be possible to physically fabricate in a given time. Validation method shows that synthetized images are as good as real spoofs considering their quality.**

***Index Terms*—Biometrics, Presentation Attack Detection, style transfer, Deep learning, Generative Adversarial Networks, Presentation Attack Instruments**

I. Introduction

Before Biometric system deployment, formal evaluations in dedicated laboratories have to be done, in order to assess their conformity to some testing scheme. These tests involve performance and presentation attack detection (PAD) testing.
The evaluation of PAD can be done through creation of physical fingerprint spoofs based on casting some materials on negative of the fingerprint used as mold [1]. This requires from testing labs to spend considerable time to physically create the presentation attack instruments (PAIs) or spoofs and acquire them with the sensor of the device under test. So, labs need to have skills to create spoofs of good quality to challenge liveness detection of fingerprint systems.
We thought that it may be interesting to be able to digitally transform genuine images to known material spoofs and help testing labs to gain time and human resources in fingerprints systems testing. We investigate how the synthetized data look like real data from the targeted material considering the quality of synthetized data.

II. Related works

The classical ways of testing biometric systems request the fabrication of physical fake fingerprints. Depending on the certification body, the process uses cooperation of the subject or not. Once, molds are created, some materials are cast on them to produce attack instruments. This way is quite "heavy" for the testing labs as it requests from them having an available number of people willing to give their personal biometric data for the purpose of a test and commits the lab to ensure data privacy related regulations such as GDPR are respected.
Hence, the use of synthetic biometric data is more and more discussed in the certification instances. Many papers deal with the creation of synthetic datasets for biometric testing. Sfinge [2] is one of the most known in this field. Many methods have followed since with the development of deep-learning methods. [3] [4] [5], [6] are based on deep learning or hybrid solutions which create high resolution biometric fingerprints.
Beside the generation of digital biometric data, some researchers have been since working on new ways of generating digital fingerprints for PAD training and testing purposes.
[7] proposed a fingerprint generalization method to help the algorithms to face digital materials unseen during the training. This method gives a TDR of 91,78%. The method proposed by Chugh *et al.* is a continuity of the universal material generator proposed by Gajawada *et al.* in [8]. [9] proposed a cross-sensors and cross-materials generalization of anti-spoofing which achieved a TDR of 87.86%.

III. Proposed method

The method we propose here is based on Wassestein GAN and particularly MWGAN [10] (Multi-marginal Wasserstein GAN). Since the introduction of Generative Adversarial Networks (GANs) [11] in 2014, many variations of this architecture have been proposed in the literature to generate fake data or to translate content from a domain to another.
Some of the most used methods for style transfer are Pix2pix [12], CycleGAN [13], StarGAN [14], etc. Some of these networks are limited by the number of domains we can learn simultaneously. So, if we want to do multi-domain we have to train as many networks as styles we want to learn.
We use the architecture proposed by Cao et al. [15]. They propose a model of multi-domains image to image translation which minimizes the Wassestein distance between the learned domains. We train the model on LivDet fingerprint datasets

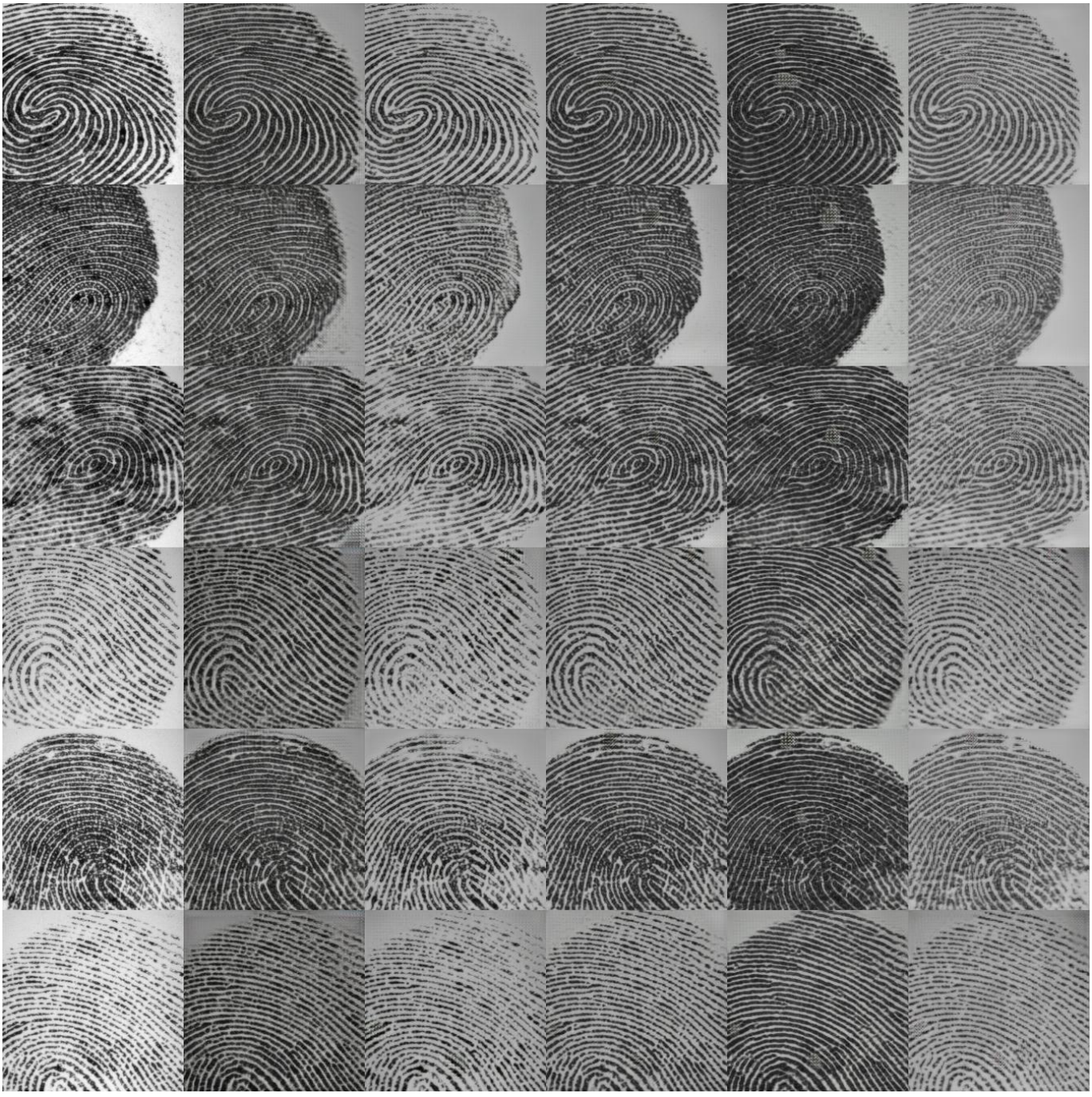

Fig. 1: Example of digital synthetized fingerprint spoofs generated. Each line comes from a different subject. Genuine images turned into spoofs in different columns: from left to right: Alive (Input), EcoFlex, Gelatin, Latex, Modasil and Wood Glue.

[16]. LivDet is an international competition of liveness detection on fingerprints. We use data from the 2013 competition from Biometrika sensor as they were of good quality and from various spoofing materials. This database includes genuine images and spoofs from Ecoflex, Gelatin, Latex, Modasil and Wood Glue. The set is composed of training set and a testing set of 2000 images each (1000 genuine images and 200 of each spoof material for each set) per used sensor. We extracted patches of 224x224 for the training. We did random cropping around the center and extracted multiples patches from each image to increase the dataset size and facilitate the training of the model.

We decide to add a data-linked term to differentiate easily the generated materials from genuine images. A matching term is used to reinforce the learning capacities of the model. As we do not know which images are selected when loading a batch for training, and genuine images and spoofs do not necessarily belong to same person, at each epoch, we perform the match between a generated batch of spoofs and respective real spoofs. As a matching score will be higher when comparing an image with itself, we think that maximizing this score will favor the similarity between the synthetically generated spoofs and the physical spoofs. We use the matcher proposed by Raffaele Cappelli [1]. An overview of the proposed method is given shown at the Fig. 2. During the training, we generate a batch of images of each material and compare them to the reference images of the same material. We add the deviation from the maximum reachable value. A detailed implementation of that part is given by Algorithm 1. Fig. 1 shows example of results where the algorithm simulates the considered materials on unseen input images.

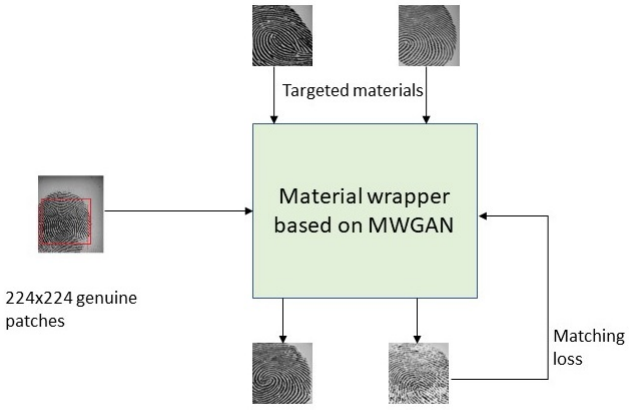

Fig. 2: Overview of the proposed method, images in the illustration do not necessary correspond to the same finger
.

[1]https://www.comp.hkbu.edu.hk/wsb2021/lecturer_details.php?lect_id=2

Algorithm 1 Attach to material

for `i < n_epochs` **do**
  for `domain in domains` **do**
    `translate to domain`
    $match\_score \leftarrow 1 - match(generated\ images, ref\ images)$
    ▷ deviation from the max value
    $loss \leftarrow loss + material\_loss$
  end for
end for

IV. RESULTS

A. Validation method

To validate the digitally synthetized fingerprint spoofs, we use quality measurement to assess the spoofness of generated data. The metric used is the NFIQ2.0 (NIST Fingerprint Image Quality) score [17]. NFIQ gives an overall score based on the usability and features of an image. Scores go from 0 to 100 (0 bad and 100 good). It is used here to see whether the digital PAIs are similar to real spoofs from that material in terms of quality.

B. Quality analysis

To validate the training of our model beyond the visual aspect of the images, we refer to the quality of the generated data using the NFIQ2.0.

Fig. 3 shows the distribution of the NFIQ score of the synthetized data and actual data for each of the 5 materials. From that figure, we can see there is a similarity between the distribution of real images and generated ones for each material and the range of covered quality scores are the same. For each material, the correlation between the quality scores of real images and digitally created images of that material gives an average value of 98,3%. The precise correlation between NFIQ scores, between real fingerprints spoofs and DSFS for all materials are given in the Table I as statistical figures.

V. DISCUSSION

This method of synthetizing digital spoofs gives good results that can make them similarly to images from real spoofs based on quality analysis. However, the current state of the art in digital fingerprint spoofs synthesis and this study show that the synthetized data could be regarded as "new materials" as they do not fully reach the targeted materials.

The observed differences with the real spoofs from targeted materials can come from different factors. Indeed, the data-linked term is a matching score based on extraction of minutiae. During the first epochs of the training, the network tries to make the template look more like ones from the destination material dataset. Indeed, some imperfections coming from the material itself can lead to the occurrence of some features in the images that can be interpreted as minutiae. These imperfections can be unique to some materials but not only as demonstrated in [18].

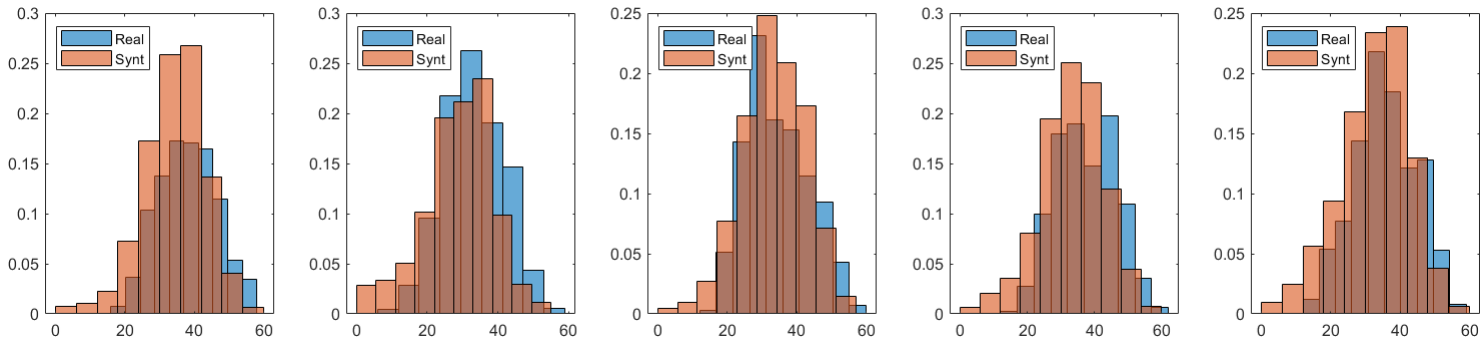

Fig. 3: Distribution of NFIQ scores for real and synthetic spoofs (from left to right: Ecoflex, Gelatin, Latex, Modasil, Wood Glue)

.

Material	real images avg	real images std	synth images avg	synth images std	Pearson correlation (%)
EcoFlex	37.879	8.4408	33.842	9.0396	97.63
Gelatin	33.33	8.875	28.549	9.9905	98.6
Latex	34.445	9.0549	33.454	9.1149	98.06
Modasil	36.874	8.8957	32.862	9.4801	98.48
WoodGlue	35.681	8.8119	32.328	10.0967	98.78

TABLE I: Statistics of the NFIQ scores of real and digitally synthetized images for the 5 materials.

VI. Conclusion and Future works

In this paper, we present a work on creation of digital fingerprint spoofs from different materials using genuine images and a multi-domain style transfer model. Results show that it gives quality similar to real spoofs from the targeted materials. This method can be used to evaluate the resistance of biometric systems to high level fingerprint spoofs. Future work will constist in deepening the qualification: Comparison to physical PAIs with matching rates, PAD metrics using different matchers and PAD algorithms.

VII. Acknowledgement

This work is supported by Fime SAS and the French National Association for Research and Technology (ANRT).

References

[1] K. Karampidis, M. Rousouliotis, E. Linardos, and E. Kavallieratou, "A comprehensive survey of fingerprint presentation attack detection," *Journal of Surveillance, Security and Safety*, vol. 2, no. 4, pp. 117–161, 2021.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Synthetic fingerprint generation," *Handbook of fingerprint recognition*, pp. 271–302, 2009.

[3] A. B. V. Wyzykowski, M. P. Segundo, and R. de Paula Lemes, "Level three synthetic fingerprint generation," in *2020 25th International Conference on Pattern Recognition (ICPR)*. IEEE, 2021, pp. 9250–9257.

[4] V. Mistry, J. J. Engelsma, and A. K. Jain, "Fingerprint synthesis: Search with 100 million prints," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2020, pp. 1–10.

[5] K. Bahmani, R. Plesh, P. Johnson, S. Schuckers, and T. Swyka, "High fidelity fingerprint generation: Quality, uniqueness, and privacy," in *2021 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2021, pp. 3018–3022.

[6] S. Seidlitz, K. Jürgens, A. Makrushin, C. Kraetzer, and J. Dittmann, "Generation of privacy-friendly datasets of latent fingerprint images using generative adversarial networks." in *VISIGRAPP (4: VISAPP)*, 2021, pp. 345–352.

[7] T. Chugh and A. K. Jain, "Fingerprint spoof generalization," *arXiv preprint arXiv:1912.02710*, 2019.

[8] R. Gajawada, A. Popli, T. Chugh, A. Namboodiri, and A. K. Jain, "Universal material translator: Towards spoof fingerprint generalization," in *2019 International Conference on Biometrics (ICB)*, 2019, pp. 1–8.

[9] S. A. Grosz, T. Chugh, and A. K. Jain, "Fingerprint presentation attack detection: A sensor and material agnostic approach," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*, 2020, pp. 1–10.

[10] J. Cao, L. Mo, Y. Zhang, K. Jia, C. Shen, and M. Tan, "Multi-marginal wasserstein gan," in *Advances in Neural Information Processing Systems*, 2019.

[11] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial nets," in *Advances in Neural Information Processing Systems*, Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, and K. Weinberger, Eds., vol. 27. Curran Associates, Inc., 2014. [Online]. Available: https://proceedings.neurips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf

[12] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, "Image-to-image translation with conditional adversarial networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, July 2017.

[13] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks," in *Computer Vision (ICCV), 2017 IEEE International Conference on*, 2017.

[14] Y. Choi, Y. Uh, J. Yoo, and J.-W. Ha, "Stargan v2: Diverse image synthesis for multiple domains," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2020, pp. 8188–8197.

[15] J. Cao, L. Mo, Y. Zhang, K. Jia, C. Shen, and M. Tan, "Multi-marginal wasserstein gan," *Advances in Neural Information Processing Systems*, vol. 32, 2019.

[16] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. L. Marcialis, F. Roli, and S. Schuckers, "Livdet 2013 fingerprint liveness detection competition 2013," in *2013 International Conference on Biometrics (ICB)*, 2013, pp. 1–6.

[17] O. Bausinger and E. Tabassi, "Fingerprint sample quality metric nfiq 2.0," in *BIOSIG*, 2011.

[18] A. Wone, J. D. Manno, C. Charrier, and C. Rosenberger, "Impact of environmental conditions on fingerprint systems performance," in *2021 18th International Conference on Privacy, Security and Trust (PST)*, 2021, pp. 1–5.