A Look At Non-Cooperative Presentation Attacks in Fingerprint Systems

Emanuela Marasco[1], Stefany Cando[1], Larry Tang[2], Luca Ghiani[3] and Gian Luca Marcialis[3]
[1] George Mason University - Center for Secure and Information Systems - U.S.
[2] George Mason University - Department of Statistics - U.S.
[3] University of Cagliari - Department of Electrical and Electronic Engineering - Italy
e-mail: {luca.ghiani, marcialis}@diee.unica.it, {emarasco, scando,ltang1}@gmu.edu

***Abstract*— Scientific literature lacks of countermeasures specifically for fingerprint presentation attacks (PAs) realized with non-cooperative methods; even though, in realistic scenarios, it is unlikely that individuals would agree to duplicate their fingerprints. For example, replicas can be created from finger marks left on a surface without the person's knowledge. Existing anti-spoofing mechanisms are trained to detect presentation attacks realized with cooperation of the user and are assumed to be able to identify non-cooperative spoofs as well. In this regard, latent prints are perceived to be of low quality and less likely to succeed in gaining unauthorized access. Thus, they are expected to be blocked without the need of a particular presentation attack detection system. Currently, the lowest Presentation Attack Detection (PAD) error rates on spoofs from latent prints are achieved using frameworks involving Convolutional Neural Networks (CNNs) trained on cooperative PAs; however, the computational requirement of these networks does not make them easily portable for mobile applications. Therefore, the focus of this paper is to investigate the degree of success of spoofs made from latent fingerprints to improve the understanding of their vitality features. Furthermore, we experimentally show the performance drop of existing liveness detectors when dealing with non-cooperative attacks and analyze the quality estimates pertaining to such spoofs, which are commonly believed to be of lower quality compared to the molds fabricated with user's consensus.**

***Keywords*— Liveness Detection, Latent Fingerprints, Non-Cooperative Attacks, Spoofing**

I. Introduction

Biometric authentication based on fingerprint identification has been successfully deployed in several high security applications such as border control, passports, visas and access control systems. Therefore, protecting the security of fingerprint recognition systems is of paramount importance [1], [2]. Attacks to these systems can be carried out using finger marks left on random surfaces with the owner being unaware that the print has been stolen and replicated. In Germany, 2008, a hacker group known as the Chaos Computer Club, lifted the country's minister's fingerprint off a water glass that he had left behind after delivering a public speech at a local university. The print was then copied by the hackers and reproduced in molded plastic 4,000 times [1]. Similarly, in 1970, Herm Wiggins, a San Diego police officer, decided to create his own fingerprint file by using fingerprints that where left on his patrol car after performing body searches on people in the streets. In the literature on biometrics, several vulnerabilities of fingerprint systems have been highlighted. An artifact carrying a print of a legitimate user can be presented to a sensor in order to gain unauthorized access [3], [4]. Moreover, an attacker could also use an artificial biometric trait to create a new identity [5]. Other scenarios, involve the use of artificial fingers, where fingerprint ridges are inscribed on materials such as gelatin, silicone, play-doh, etc [5]. Multiple studies have shown that these type of artificial fingers, when realized with cooperation of the individual, are very effective in breaking commercial systems. Fabricating

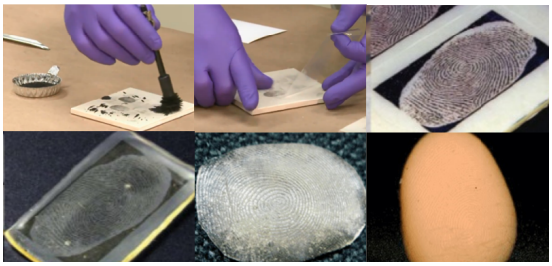


Fig. 1. Acquisition process of fingerprints left on random surfaces.

effective spoofs from latent prints is much more complex than obtaining them by users' consensus. Thus, it is expected that the quality of a replica from a latent fingerprint would be lower than the one obtained with cooperative methods. However, a presentation attack is more realistic if performed with such spoofs since it is very unlikely that a person will consent to produce a mold carrying his / her fingerprint. Moreover, none have showed so far that a latent print can break a fingerprint verification system, especially if such system is integrated on mobile devices, where a very low False Rejection Rate (FRR) must be considered. The lowest error rates reported for Presentation Attack Detection (PAD) on spoofs from latent currently involve frameworks based on CNNs [6], [7], [8]. However, the impracticality of using pre-trained networks on smaller computational form factors necessitates the need to learn smaller network architectures. The quandary now is that smaller networks' architectures cannot produce powerful enough representations[9].

The problem faced in this paper pertains to a dataset and

[1] http://www.slate.com/articles/technology/future_tense/2015/02/future_crimes_excerpt_how_hackers_can_steal_fingerprints_and_more.html

algorithm bias of existing anti-spoofing countermeasures due to the spoofing process (non-cooperative vs. cooperative). The focus of this research is on liveness detectors trained on cooperative spoofs and tested on non-cooperative ones. We experimentally investigate the correlation pertaining to matching spoofs realized based on latent fingerprints and live fingerprints; we also analyze the related quality of fake samples. We then examine the effectiveness of the attacks when the matcher's performance is set to be user-friendly and has operational points set at 0% False Rejection Rate (FRR), 1% FRR, 5% FRR and 10% FRR. Starting from these results, we want to propose, on the basis of statistical relationships, the liveness score, match score, and quality score appropriately modeled to integrate a verification-liveness detection model that will strongly reduce the probability of spoof acceptance and minimize the False Acceptance Rate (FAR) of the system, and possibly its FRR as well. Moreover, we study some of the current presentation attacks detection approaches and we analyze their efficiency to detect and differentiate latent spoof prints from live fingerprints.

Section 2, summarizes the related work in this field, and the efforts made to enhance fingerprint detection mechanisms. Section 3, discusses the experiments carried out to specifically analyze fingerprint presentation attacks realized with non-cooperative approaches. Last, Section 4, draws conclusions and discusses future research.

II. Related Work

Fingerprints are easily deposited on surfaces such as glass, metal, or polished stone by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges [5]. Prints are left under supervised conditions while marks are left in an uncontrolled environment. Often, prints are only partially visible or not visible at all without the use of specialized fingerprint processing methods and equipment. Three methods for revealing fingerprints are commonly used:

- The first method is based on latent fingerprints lifted with powder. The fingerprint left on a surface is placed on a transparency and it is visualized by powdering with a brush. The powder is removed from the background using scotch tape[2]. This lifted print is placed on the sensor.
- The second method is based on a photolithographic PCB (Printed Circuit Board) mold. The fingerprint is placed on a transparency and enhanced by brushing with a black powder. Then it is photographed by using a digital camera and printed on a transparency to create a mask for etching the PCB. The mask is placed on the circuit and exposed to UV light. The plaster cast of the fingerprint is filled with liquid silicon rubber to create a wafer thin gummy and it is attached to a live finger before being placed on a sensor.
- The third method is based on a recent advancement that shows the unique ability to lift latent fingerprints from various surfaces and visualize them under daylight within 30 seconds. Such a fast recognition is based on an electrospun nanofiber mat [10]. Fingerprint reactivation can be carried out with simple techniques such as breathing on the sensor, placing a water filled plastic bag or brushing graphite powder on the sensor have been used to reactivate latent fingerprints deposited on a sensor.

[2]https://www.youtube.com/watch?v=$_PPsRLONghAt = 102s$

Presentation Attacks (PAs) have been detected by either gathering further evidence of vitality of the subject (e.g. sensing blood circulation, or fluids - perspiration patterns - secreted when touching surfaces) or by passive methods detecting the presence of known materials (e.g. material structure, lack of high-resolution detail) [11], [12]. Several software-based methods, including Fourier Transform (FT), Local Binary Patterns (LBP), Binarized Statistical Image Features (BSIF), Local Phase Quantization (LPQ), Weber Local Image Descriptor or Histograms of Invariant Gradients (HIG), have been investigated for PAD [13], [14], [15], [16].

Recently, deep learning approaches have been applied; however, presented techniques were largely hybrid (combined with other classification techniques) and no pure CNNs have been evaluated for this task shedding light onto robustness to new fabrication materials [17], [7], [18]. Previously, Menotti *et al.* derived an efficient spoof detection system through deep representations. They first learn a suitable CNN architecture, which is determined through a random search procedure involving hyper-parameter optimization of the network. Then, the candidate architecture is evaluated by executing linear SVM on the deep representation obtained by the considered net. Frassetto *et al.* have examined fingerprint liveness detection using CNNs and LBPs, however they employ a hybrid approach feeding the netâs output into an SVM rather than exploiting the power of deep networks only with best reported accuracy of 95.2% using 50,000 samples for training using LivDet 2009, 2011 and 2013 datasets [6]. Apart from classical classification nets, also metric-based deep Siamese networks have been evaluated learning a distance metric enforcing live-spoof pairs to be of higher distance than live-live pairs. This is useful for attended enrollment scenarios where a live gallery image is available (e.g. trusted-source fingerprint reference on the passport chip). Experiments revealed remarkable accuracy for all Convolutional Neural Networks (CNNs) CaffeNet (96.5%), GoogLeNet (96.6%), Siamese (93.1%), good material robustness (max. 5.6% diff.) but weak sensor-interoperability [19].

The methods discussed above do not specifically address the problem of performance degradation of a liveness detector trained on cooperative attacks and tested on non-cooperative ones. Generally, current anti-spoofing measures tested on spoofs made from latent in the testing databases made available from LivDet 2013 present very high error rates. In 2018, reasonable error rates are reported by Chugh *et al.* where Ferrfake is 0.34% on Biometrika LivDet 2013 and 0.68% on Italdata LivDet 2013 both at Ferrlive of 1% [8]. This approach uses CNNs trained on local patches centered and aligned using minutiae location and orientation, respectively. However,

most of these networks require state-of the-art GPUs to work even in simple feed forward modes [9]. The computational requirement of these networks do not make them easily portable. Beyond exploring deep networks, Frassetto *et al.* reached a good accuracy through dataset augmentation [7]. However, sufficient computational power is required for the augmented datasets [7].

III. Liveness or Presentation Attacks Detection Algorithms used in this Analysis

We consider three different mechanisms to extract the liveness of the fingerprints and see if the latent replicas can break the system when this detection mechanisms are in place. *Binarized Statistical Image Features (BSIF)*, is a textural analysis algorithm where local image patches are linearly projected into a subspace whose basis vectors are obtained from images by using Independent Component Analysis (ICA); coordinates of each pixel are thresholded and a binary code is computed. Such a value represents the local descriptor of the image intensity pattern in the neighborhood of the considered pixel [20]. The set of filters is learned from a training set of natural image patches via ICA by maximizing the statistical independence of the filter responses [21]. The fingerprint representation is, therefore, obtained by learning, instead of manually tuning, based on statistical properties of the input signal; this procedure provides flexibility to the designed descriptor [13]. *Local Binary Pattern (LBP),* was originally developed for two-dimensional texture analysis obtaining excellent results [22]. In a circular neighborhood of each pixel of a gray scale image, it compares the surrounding pixels with the central pixel, hence encoding a predefined set of texture templates or micro-patterns. The histograms of these patterns are used as an image descriptor. LBP combines structural (basically a filter capable of identifying structures such as lines and borders) and statistical (micro-structures distribution) information. *Local Phase Quantification (LPQ),* is a blur-tolerant textural descriptor. It works on the frequency domain but, unlike other algorithms that analyze the image spectrum in high frequencies, LPQ focuses on the lower frequencies [23]. Once the local spectrum is computed using a short-term Fourier transform in a local neighbourhood, the function values are sampled in four pre-set frequency values. In the short-term Fourier transform, the filter function is chosen to be a windowed complex exponential. From the sign of the real and imaginary parts of these four values, eight binary coefficients are derived. These allow to represent the phase information with an integer value in the range [0, 255]. The occurrences of these values are collected into a histogram which is used as the LPQ feature vector [14], [5].

IV. Experimental Investigation

We analyzed match scores between live fingerprints and spoofs obtained using non-cooperative methods. The experiments were carried out using the LiveDet 2013 Biometrika Test Dataset (see Tab. 1), which contains 1000 live fingerprint images and 1000 spoof images. The acquisition with this optical sensor makes our analysis from an optimistic perspective given that in mobile applications images would be of worst quality. Spoofs were fabricated by materials such as ecoflex, gelatine, latex, modasil, and wood glue, see Fig. 2 [24]. To the best of our knowledge, databases for training and evaluation of liveness detectors on images acquired through fingerprint sensors embedded in mobiles have not been collected. This research direction is currently challenging anti-spoofing solutions. The data set used in this analysis includes only live fingerprint images with corresponding spoofs for a total of 700 live images and 200 images per material. Match scores were extracted with Neurotechnology VeriFinger 9. It was unexpected that spoof replicas created from latent fingerprints would obtain high match scores. In Fig. 3 (a), we notice that setting a threshold that rejects all impostors' scores would still cause multiple spoof values pass the threshold and break the system. Furthermore, we can also see that it is very difficult to set a threshold that would discriminate the spoof prints without affecting the acceptance of live genuine prints.

Based on Tab. 2, we observe a drop in performance of the current identification mechanisms when spoof prints are presented to the system; even when operational points are set to 5% and 10% FRR, we still have a concerning False Acceptance Rate of spoof prints.

In order to experimentally verify the common believe that the quality of images coming from latent print-based spoofs is low, we computed the quality scores pertaining to live fingerprints versus those extracted from spoofs realized with non-cooperative methods. Quality scores were estimated using NFIQ 2.0, for all live print images and non cooperative spoof images. NFIQ 2.0 is a classifier that uses global and local features to predict the quality of an input. Some of the features of this classifier includes minutiae count, orientation coherence, orientation certainty, frequency analysis, quality at minutiae locations, histogram of local features, and mean and standard deviation of local features [25] [3].

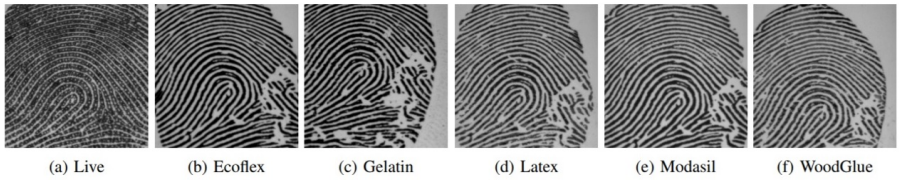
Despite the fact that the quality score of spoof print replicated from latent fingerprints are expected to be low, Fig. 3 b. shows that the scores obtained from the spoofed replicas are higher than the live prints. This can be explained by the fact that spoofs from latent print must pass a preliminary process of image improvement by hand and use appropriate image processing tools. Therefore, the quality score as intended by NIST and the research community is not able to detect or adequately evaluate the correspondent quality of latent print-based spoofs.

On the basis of what reported, image quality does not affect the match score directly. This is shown in Fig. 4 (a) and (b). Therefore, we can not use quality as a measure to differentiate live from spoof prints. Fig.4 (c) and (d) compare the match scores and the average of liveness scores obtained using

[3]NFIQ 2.0 Specifications: https://www.nist.gov/sites/default/files/documents /2016/12/06/15$_o lsen_2 0160504_i bpc_n fiq 2.0 - features_o lsen.pdf$

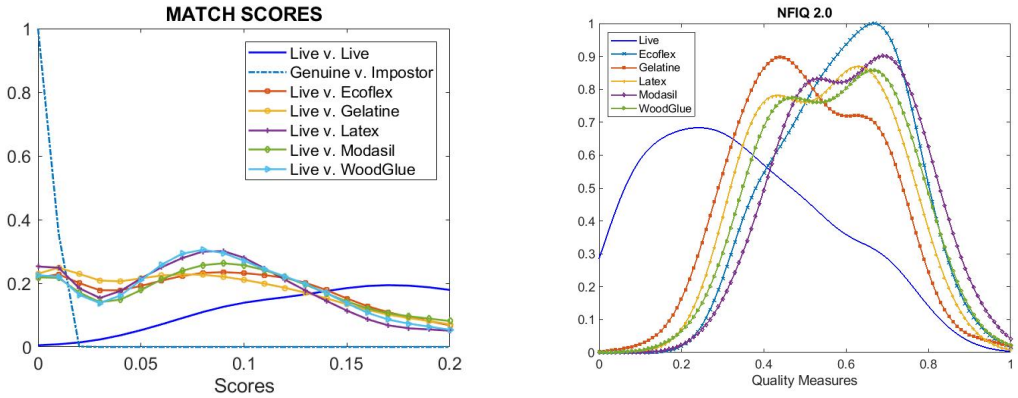
Dataset Description					
Sensor	Model No.	Resolution (dpi)	Image size	No. of Images	
				Live	Spoof
Biometrika	FX2000	569	315 x 372	1000	1000
Italdata	ET10	500	640 x 480	1000	1000

Table 1. LiveDet2013 Biometrika Dataset description.



(a) Live (b) Ecoflex (c) Gelatin (d) Latex (e) Modasil (f) WoodGlue

Fig. 2. Materials used to fabricate the spoof samples taken from LivDet 2013 databases.



(a) (b)

Fig. 3. Using the LivDet2013 Biometrika Test Dataset we calculated: (a) Probability density distribution of genuine match scores using live and spoof prints were compared with the scores obtained from impostors. The graph represents the behavior of the system without any liveness detectors, which results in an overlap within the live match scores and the spoof prints. (b) Probability density distribution of the quality scores obtained from the live and spoof fingerprints images using NIST NFIQ 2.0.The same experiment was replicated using the LivDet2013 Italdata Test Dataset, where we found similar results as the ones represented above.

Performance of Fingerprint Detection System based on FAR				
Material	0% FRR (Score >0)	1% FRR (Score >0.037)	5% FRR (Score >0.069)	10% FRR (Score 0.088)
Ecoflex	100 %	73.75 %	59.50 %	47.80 %
Gelatine	100 %	71.50 %	54.30 %	43.95 %
Latex	100 %	75.05 %	57.35 %	44.10 %
Modasil	100 %	76.99 %	62.25 %	50.65 %
Wood Glue	100 %	77.60 %	60.55 %	46.05 %

Table 2. False Acceptance Rate of user-friendly devices where the identification systems have operational points set to be 0% FRR, 1% FRR, 5% FRR and 10% FRR.

mechanisms such as BSIF, LPQ, and LBP. From the graph we can see that materials like Gelatine and Wood Glue can reach high Liveness scores; moreover, such spoofs will be able to break the system even if we use these current mechanisms to detect the liveness of the prints. Last, Fig.4 (e) and (f) show the comparison within quality and liveness scores; here we can observe that quality does not affect the liveness scores. However, liveness scores of certain prints are very high, which means that the liveness mechanisms being used are not effectively able to identify the spoof prints from the live prints. It is also important to acknowledge that certain live prints have a very low liveness score, which may result in such prints

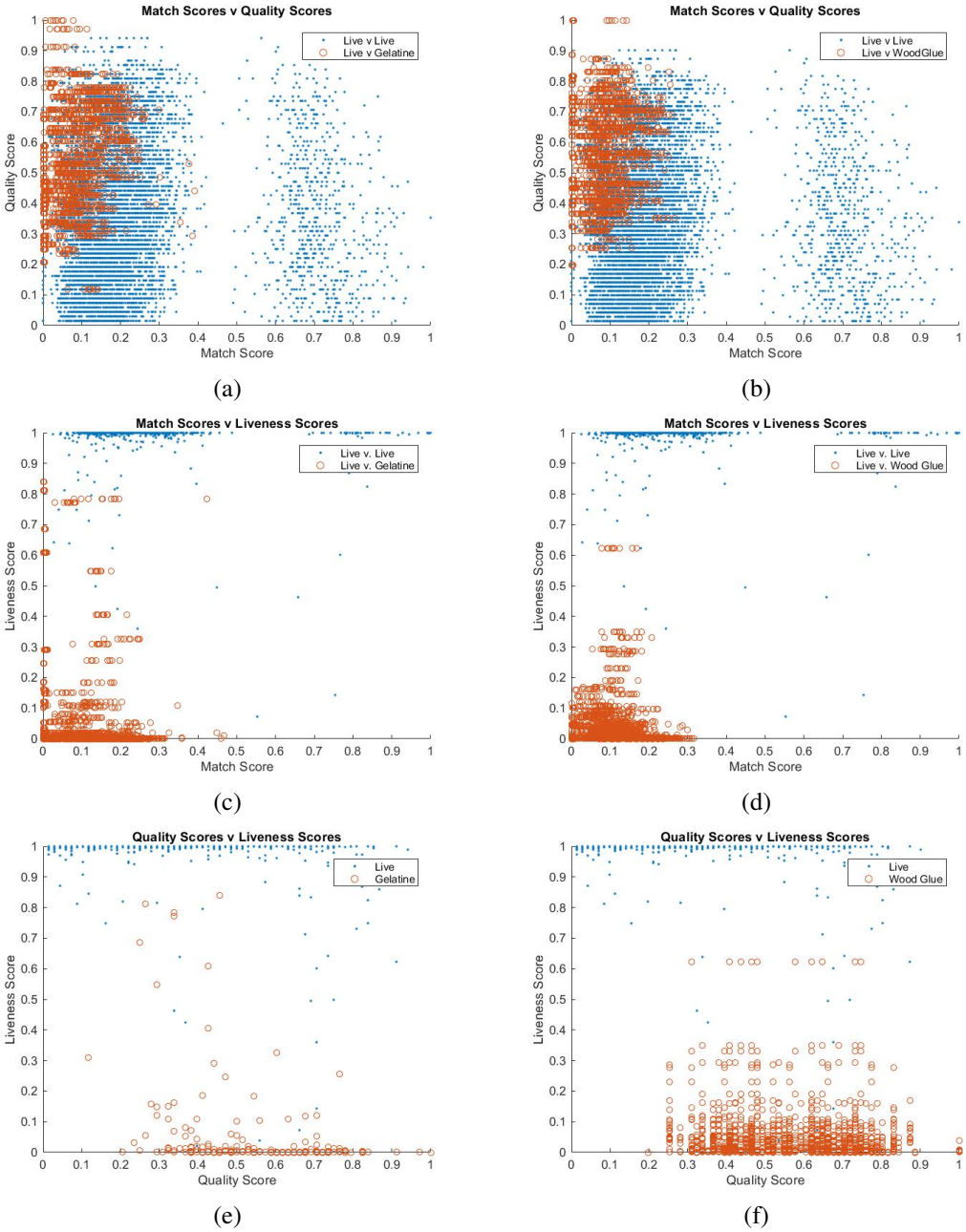


Fig. 4. Comparison between Quality, Match, and Liveness scores of spoof and live fingerprints. Focused on critical cases involving materials like Gelatine and Wood Glue specifically, as the prints made from these materials are more likely to deceive the identification system. Similarly, certain spoof prints made of materials like modasil and latex also show and overlap with live prints; however the results were not as critical as the cases shown above. The liveness scores were acquired using LPQ; algorithms such as LBP and BSIF presented similar results.

being labeled as spoofed and rejected by the system. Finally, we estimated the pairwise correlation parameters between genuine and spoofed prints for the match and quality scores. The goal is to evaluate if a common behaviour can be identified among couples of materials, so that the knowledge of a certain one can cover the absence of knowledge about another one. This is motivated by the fact that presentations attacks can be intended as an arms-race problem, where the attacker is expected to use never-seen-before material, as in the recent edition of LivDet (2015 and 2017 editions)[4]. The spoofed print materials include aforementioned Ecoflex, Gelatine, Latex, Modasil, and WoodGlue. For continuous match scores, we estimated Spearman's correlation and conducted hypothesis tests on the significance of the correlation. Since the NFIQ2 quality scores have many ties, we estimated Kendall's tau and conducted hypothesis tests on the correlation.

For the match scores, the correlation parameters are positive,

[4]See the LivDet website: http://livdet.diee.unica.it.

and the p-values for testing whether the correlation is zero are much less than 0.05. This indicates significant positive correlation among genuine prints and spoofed prints, and positive correlation among different types of spoofed prints. For the quality scores, genuine prints have significant positive correlation with spoofed prints, except for wood glue. The correlation between genuine and wood glue is not significant, with the correlation of -0.0098 and the p-value of 0.52. The correlation estimates between WoodGlue, Ecoflex, Gelatine, Latex, or Modasil are 0.0138, -0.0305, 0.0365, and 0.0194, respectively. The wood glue does not have significant correlation with Ecoflex or Modasil. The wood glue has a marginally significant correlation with Gelatine (p-value=0.047), and significant correlation with Latex (p-value=0.018). To summarize the results, for the match scores, there is a statistically significant positive correlation among genuine prints and spoofed prints, and among different types of spoofed prints. For the quality scores, genuine prints have significant positive correlation with spoofed prints, except for wood glue. Since the quality scores were developed from genuine prints, more research needs to be conducted regarding quality scores for matching spoofed prints, especially spoofed prints from wood glue. The above analysis allows us to conclude that fingerprint presentation attacks detection can be strictly considered as an arms-race problem, as expected: the knowledge about a certain material is not relevant when dealing with never-seen-before materials.

V. Conclusions

In this paper, we investigated the statistical relationships between match scores, quality scores and liveness scores of fingerprint spoofs created from latent fingermarks. The purpose of our analysis was to see at which extent a realistic attack, using non-cooperative methods, would be able to deceive the identification system. We challenged the claim that spoofs from non-consensual methods are expected to be of low quality, and that current liveness detectors should be able to block such attacks. The results of our study led us to three basic conclusions: (1) latent print-based spoofs are able to break the current system, especially when the threshold is set to user-friendly operational points (low FRR), (2) there is no correlation between the quality and the effectiveness of the spoof, (3) spoofs made from new materials can be difficult to be detected by the system. These claims need to be further investigated using a collection of data sets of non-consensual spoofs larger than the ones used in this experiment.

Acknowledgements

Liansheng Tang would like to acknowledge the support of the Information Technology Laboratory at the National Institute of Standards and Technology, U.S. Department of Commerce. The statements, finding, and conclusions in this research, are those of the authors and do not necessarily reflect the view of NIST or the U.S Department of Commerce.

References

[1] C. C. Roberts, "Biometric attack vectors and defences," *Computers & Security*, vol. 26, no. 1, pp. 14–25, 2007.

[2] A. Sten, A. Kaseva, and T. Virtanen, "Fooling fingerprint scanners - biometric vulnerabilities of the precise biometrics 100 sc scanner," 01 2003.

[3] S. Schuckers, "Spoofing and Anti-Spoofing Measures," *Information Security Technical Report*, vol. 7, no. 4, pp. 56–62, 2002.

[4] K. Nixon, V. Aimale, and R. Rowe, "Spoof Detection Schemes," *Handbook of Biometrics*, 2007.

[5] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Comput. Surv.*, vol. 47, pp. 28:1–28:36, Nov. 2014.

[6] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Evaluating software-based fingerprint liveness detection using convolutional networks and local binary patterns," *Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, pp. 22–29, 2014.

[7] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks.," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 6, pp. 1206–1213, 2016.

[8] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: Use of minutiae-centered patches," *IEEE Transactions on Information Forensics and Security, DOI: 10.1109/TIFS.2018.2812193*, 2018.

[9] R. Venkatesan and B. Li, "Diving deeper into mentee networks," *arXiv preprint arXiv:1604.08220*, 2016.

[10] Y. Shengyang, W. CaiâFeng, and C. Su, "A release induced response for the rapid recognition of latent fingerprints and formation of inkjet printed patterns," *Angewandte Chemie International Edition*, vol. 50, no. 16, pp. 3706–3709.

[11] S. Marcel, M. Nixon, and S. Li, *Handbook of Biometric Anti-Spoofing*. Springer, 2014.

[12] S. Nikam and S. Agarwal, "Curvelet-based fingerprint anti-spoofing," *Signal, Image and Video Processing*, vol. 4, pp. 75–87, January 2009.

[13] L. Ghiani, A. Hadid, G. Marcialis, and F. Roli, "Fingerprint liveness detection using local texture features," *IET Biometrics*, vol. 6, pp. 224–231(7), May 2017.

[14] L. Ghiani, G. Marcialis, and F. Roli, "Fingerprint Liveness Detection by Local Phase Quantization," *Proc. ICPR*, pp. 1–4, November 2012.

[15] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint Liveness Detection based on Weber Local Image Descriptor," *Proc. BioMs*, pp. 1–5, 2013.

[16] C. Gottschlich, E. Marasco, A. Yang, and B. Cukic, "Fingerprint Liveness Detection based on Histograms of Invariant Gradients," *Biometrics (IJCB), 2014 IEEE International Joint Conference on*, pp. 1–7, Sept 2014.

[17] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in neural information processing systems*, pp. 1097–1105, 2012.

[18] R. Raghavendra and C. Busch, "Robust Scheme for Iris Presentation Attack Detection using Multiscale Binarized Statistical Image Features," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 703–715, 2015.

[19] E. Marasco, P. Wild, and B. Cukic, "Robust and interoperable fingerprint spoof detection via convolutional neural networks," *IEEE International Conference on Technologies for Homeland Security*, pp. 1–6, 2016.

[20] J. Kannala and E. Rahtu, "BSIF: Binarized statistical image features," *Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)*, pp. 1363–1366, 2012.

[21] A. Hyvarinen and E. Oja, "Independent component analysis: algorithms and applications," *Neural Networks*, vol. 13, no. 4, pp. 411 – 430, 2000.

[22] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, pp. 971–987, Jul 2002.

[23] J. Heikkila and V. Ojansivu, "Methods for local phase quantization in blur-insensitive image analysis," in *2009 International Workshop on Local and Non-Local Approximation in Image Processing*, pp. 104–111, Aug 2009.

[24] L. Ghiani, D. Yambay, V. Mura, S. Tocco, G. Marcialis, F. Roli, and S. Schuckers, "LivDet 2013 fingerprint liveness detection competition 2013," in *Proc. ICB*, (Madrid, Spain), pp. 1–6, June 2013.

[25] M. Olsen, "NFIQ 2.0 - Features for fingerprint quality determination," 05 2016.