Received: 10 July 2021 | Revised: 18 September 2021 | Accepted: 23 September 2021

DOI: 10.1111/1556-4029.14908

JOURNAL OF FORENSIC SCIENCES AAFS

PAPER

Criminalistics

Proactive forensic science in biometrics: Novel materials for fingerprint spoofing

Michel Saguy ME[1] | Joseph Almog PhD[2] | Daniel Cohn PhD[2] | Christophe Champod PhD[1]

[1]Ecole des Sciences Criminelles, Université de Lausanne, Lausanne, Switzerland

[2]Institute of Chemistry, The Hebrew University of Jerusalem, Jerusalem, Israel

Correspondence
Michel Saguy, ME, Ecole des Sciences Criminelles, Université de Lausanne, Lausanne, Switzerland.
Email: michel.huji@gmail.com

Funding information
This research was partially supported by the Israel Counter-Terrorism Bureau.
Open access funding provided by Universite de Lausanne.
WOA Institution: Universite de Lausanne
Blended DEAL: CSAL

Abstract

Motivated by the need to prepare for the next generation of fingerprint spoofing, we applied the "proactive forensic science" strategy to the biometric field. The working concept, already successful in a few fields, aimed at adopting the sophisticated criminals' way of thinking, predicting their next move so that the crime-fighting authorities can be one step ahead of them and take preventive measures, against biometric spoofing in this instance. This strategy involved the design, production, and characterization of innovative polymeric materials that could possibly serve in advanced fingerprint spoofs. Special attention was given to materials capable of fooling fingerprint readers equipped with spoof-detecting abilities, known as "Presentation Attack Detection" (PAD) systems and often referred to as liveness detection. A series of direct cast fake fingerprints was produced from known commercially available spoofing materials, and was functionally tested to compare their performance with that of spoofs produced from the new polymers. The novel materials thus prepared were hydrogels based on polyethylene glycols (PEGs) that were chain-extended. They showed good performance in deceiving security systems, considerably better than that of spoofs produced from commercial materials, and are, therefore, good spoofing candidates that law-enforcement authorities should be aware of.

KEYWORDS
proactive forensic science, biometrics, presentation attack detection, PAD, fingerprint spoofing, liveness, hydrogels, polyethylene glycol, PEG

Highlights

- In this research, we applied the "proactive forensic science" strategy to biometrics.
- This strategy involved the design, production, and characterization of innovative polymeric materials as potential advanced fingerprint spoofs.
- Methodically modified PEG-hydrogels, thus, prepared showed good performance in deceiving fingerprint readers.

1 | INTRODUCTION

The contest between crime and the law often takes the format of a vicious circle as in the case of new psychoactive substances that regularly appear on the market when not yet covered by legal provisions. It is only after they have been identified and characterized by forensic laboratories that they are added to the list of illegal substances in various countries' Illicit Drugs Acts. However, in the meantime, newer compounds appear and the cycle continues [1]. A similar situation prevails in the biometric domain, especially in fingerprint recognition, with their increased use in controlled-access systems throughout the past decade [2–6].

Despite their numerous advantages, fingerprint recognition systems are vulnerable to a variety of attacks. One of them, the presentation of fingerprint spoofs, was proven successful [7,8]. Moreover, certain dedicated websites such as the Chaos Computer Club at https://www.ccc.de/en/ provide instructions on how to fake fingerprints (and published on http://biometrics.mainguet.org/ website) [9]. Indeed, several anecdotal cases of fraud by means of spoof fingerprints have been reported [10–14], all used by individuals for the purpose of impersonating or deceiving controls.

The vulnerabilities of current fingerprint readers have been studied by several research groups who demonstrated that many sensors can be fooled by fake fingerprints [15–18]. Fingerprint patches made of commercially available materials such as silicone, latex, or gelatin are among the best-known spoofs, producing "gummy fingers" [7,8,16].

Consequently, developers of fingerprints sensors have designed countermeasures [19,20] and biometric systems' manufacturers have added anti-spoofing capabilities, presentation attack detection (PAD) systems, to their devices. Many of them are hardware-based, several rely on the electrical properties of the skin, some are based on multispectral imaging, and a few have added a separate sensor for that purpose [21–25]. Others are software-based, trying to identify the fakes by image analysis, nowadays using convolutional neural networks (CNN) [21,26–28]. The latter, apparently, is more susceptible to being fooled by high-quality spoofs made of superior mimicking materials. This work focuses on fingerprint-readers equipped with hardware-based PADs, especially optical and solid-state sensor readers, as they are the most widespread devices [29].

The known spoofs are quite efficient and easy to produce, but from the criminal's point of view, they suffer from several shortcomings such as short shelf life and poor chemical resistance. In addition, some of them, e.g., silicone replicas, are effective only against certain readers, primarily the optical ones [22].

We anticipate that the sophisticated criminals may try to produce more advanced spoofs, undetectable by the new PADs [30,31]. Furthermore, the organized-crime groups have the resources and the technological know-how that enable them to design and synthesize such advanced and efficient new spoofing materials [32–35].

This research stems from the proactive forensic strategy already introduced in 2014 [36], with the goal of enabling crime-fighting organizations to be one-step ahead of "educated" criminals, in this case, fingerprint forgers. This preemptive strategy, often referred to as "forensic intelligence," has already been successful in combating cyber-crime [37] and has shown potential also within the battle against new designer drugs [1,38]. With the growing use of biometrics, we suspect that the next war on terrorism and organized crime with regard to identity theft and fraud will be conducted mainly against biometric spoofing.

Following this proactive approach, we aimed at producing new fingerprint spoofs from new materials specifically designed and synthesized for this purpose.

The mimicking material should enable exact replication of the pattern and the relevant properties of the fingers without any machine-distinguishable defects. Hence, the material has to be able to reproduce the morphology and the fine details of the fingertip, while at the same time, be compatible with a live finger and show similar physical or optical properties. Only a few properties of the finger are essential when applied to the reader, most importantly its topography, its hardness, and its electrical conductivity. Hydrogels were selected as a promising material for the purpose for the following reasons: While being insoluble in water, hydrogels are distinguished by their ability to contain water [39], which contributes to the polymer's conductivity. Additionally, like many other polymers, hydrogels can be tailored to meet specific requirements based on their exact composition, commonly used for various biomedical applications [40,41]. The properties of these materials depend on their building blocks and on the preparation procedures and can be extensively modified.

Many of the most widely used hydrogels are based on polyethylene glycol (PEG), also known as polyethylene oxide (PEO). Hydrogels based on PEG derivatives are likewise widely applied [42].

Aiming at producing a series of high-quality fingerprint spoofs, which will successfully deceive selected PAD systems, this research focused on synthesizing novel spoofing materials based on PEGs and PEG derivatives, chain-extended to produce new polymers. The PEG is the main component of the backbone and its high hydrophilicity is restrained and controlled by introducing hydrophobic functional groups to the polymer.

PEG-based spoofs were produced by the direct cast method [21,43] under the assumption that the criminals involved in "high-quality" spoofing will usually get the cooperation needed. This method was chosen due to the fact that it generally produces better impressions [15,29,43].

Due to the sensitivity of the subject, we have chosen not to disclose detailed information such as the specific chemicals involved and the devices tested.

2 | MATERIALS AND METHODS

2.1 | Reagents and compounds preparation

All the new polymers were based on polyethylene glycols (PEGs) or analogous diamines commercially available chemicals, purchased from Sigma – Aldrich Israel. Syntheses were conducted based on a

variety of homologous hydrogels, with molecular weights ranging from 400 to 20,000 Da.

All syntheses were performed by a one-pot reaction, producing polyurethane, polyurea, and polyamide hydrogels. The different polymers were investigated and characterized, from the molecular level and up to the functional level, according to the requirements defined. Various analyses were conducted: chemical analysis by H^1NMR and FTIR, molecular weight by GPC, morphology by DSC, water uptake by the gravimetric technique, mechanical properties using a universal testing machine (UTM), and a hardness tester. Electrical resistance was measured by a high-sensitivity multimeter.

2.2 | Artifacts and database production

A collection of artificial fingerprints was created by the direct cast method from 13 volunteers' fingers, producing 78 silicone molds of "cooperating fingerprint-donors." The database was built both digitally and physically. Six fingers of each of the volunteers were enrolled using three different fingerprint readers, two optical and one multispectral, each of the three readers equipped with a different proprietary presentation attack system (PAD).

Following the enrolment, silicone molds were fabricated using a commercial dental impression-material, by applying the molding material on the volunteers' fingers. Subsequently, different replicas of the fingerprints were produced by casting the spoofing material into the molds.

The hydrogel spoof samples were prepared by solvent casting from an organic solvents solution. Replicas made from known spoofing materials, commercially available silicone, polyurethane, and latex similar to some of those used in the LivDet competitions [44–48], were produced to compare their performance and deceiving ability to that of the new spoofs.

2.3 | Biometric instruments and systems

The new spoofs were functionally tested using the three capturing devices, verifying the readability of the spoofs and the response in PAD mode. Preliminary PAD testing was also conducted on a fourth system that has a different PAD system and was acquired in the course of the research.

2.4 | Functional evaluation and analysis

Functional tests were conducted on the database created using the spoofs produced. First, identification of the spoofs was carried out using the Neurotechnology's Neurotec Biometric 6.0 (VeriFinger) software and the three readers.

Each sample was then tested in the enrolment mode with each of the three readers with some preliminary tests with the fourth reader, using their corresponding software and their PAD system. The Neurotec software's anti-spoofing feature was too limited; it did not fully support the PAD system of the readers.

The various artifacts were then tested for spoofing by applying them on the different readers and recording the response of the PAD systems, three times each, setting the detection threshold level to the default values. The rate of spoofing success was noted as the False Acceptance Rate (FAR), according to the "liveness score" attained.

Additionally, a similar functional performance analysis was conducted by testing artifacts on one commercial software-based PAD. This latter system was trained using LivDet databases [44–46]. Several images of the various spoofs were examined by the software and their "liveness" score was recorded.

2.5 | Quality measure

The quality of the various spoofs, both commercially based and novel-hydrogels, was determined using the NIST quality engine NFIQ 2 [49] after reformatting the images (BMP) to meet the requirements of the software. NFIQ is a fingerprint image quality algorithm issued by NIST in 2004; an upgraded version, the NFIQ 2 [50], was released in 2016 and used in this research.

3 | RESULTS

Among the various candidates available, we chose polyethylene glycol (PEG) [1] as the backbone (Figure 1).

PEGs, differing in their molecular weights, were chain-extended using hexamethylene diisocyanate (HDI) [2] thus producing new polymers. The chemical reaction is shown in Figure 2.

Similarly, Jeffamine ED [3], analogous diamines, were chain extended using HDI [2], producing a comparable polyurea-hydrogel, as shown in Figure 3.

Several series of high-quality spoofs were produced in the silicone molds, one is shown below in Figure 4. The spoofs were

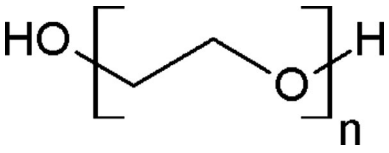

FIGURE 1 Polyethylene glycol (PEG)

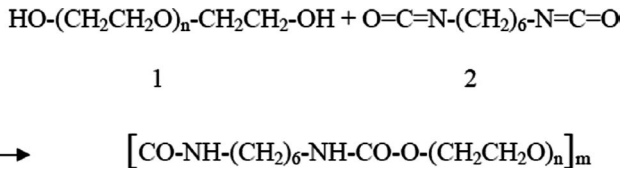

FIGURE 2 Poly-PEG-urethanes formation

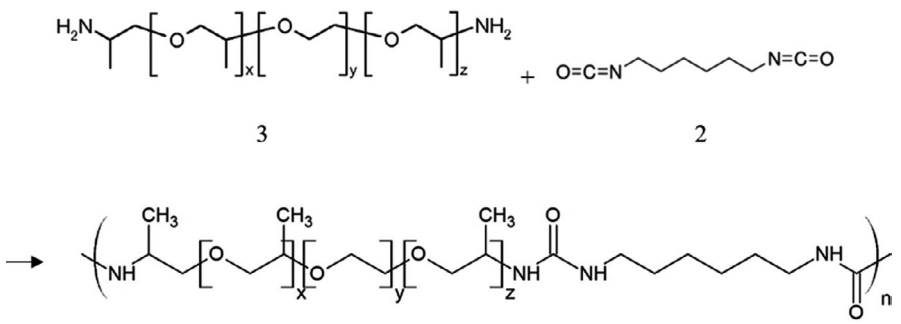

FIGURE 3 Poly-Jeffamine-urea formation

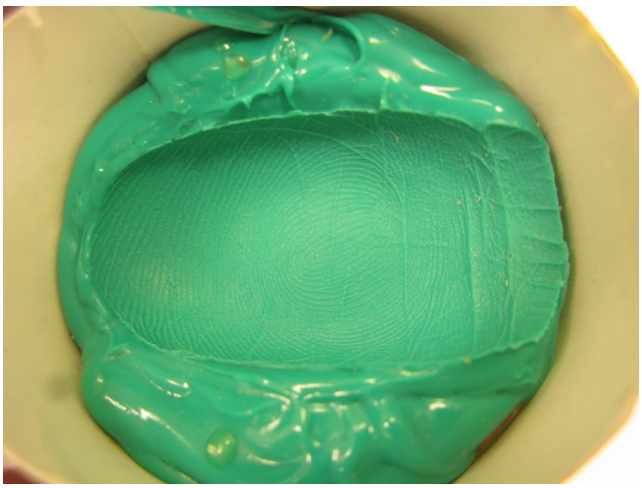

FIGURE 4 A silicone mold

FIGURE 5 A hydrogel spoof

produced via the direct cast method that generated molds of high quality, thereby, enabling good replication of the fine details of the fingers' topography. One of the hydrogel spoofs is shown in Figure 5.

The PEG-based hydrogels exhibited good characteristics and improved functional properties.

TABLE 1 Hardness and resistivity of selected hydrogels versus human skin properties

	Shore A	Resistivity (MΩ)
Human	3~18	4~27
Hydrogel #1	9.7±0.6	16.8±3.6
Hydrogel #2	23.3±2.3	45.1±7.4

Referring to the main properties required, the leading new materials achieved an adequate electrical resistivity of about 15–50 MΩ, expressing the conductivity, and a hardness similar to that of a human finger, Shore A ranging from 9 to 26, as measured in the laboratory and shown in Table 1. The conductivity, although being low, still enabled reading by the device when necessary.

The two selected hydrogels showed good functional properties as detailed below, one somewhat better than the other although its properties relatively inferior, due to the different functional groups within the polymer and their frequency along the chain, the first based on the urea linking groups and the second on urethane groups.

When tested by the biometric readers, the image quality of the spoofs was not very high, due to the presence of air bubbles entrapped in the product. The quality was later improved as detailed hereafter. All of them, however, were readily recognized by the readers and received high scores upon biometric identification, 48 being the default and recommended minimum score, as presented in Figure 6 below.

3.1 | Biometric testing and evaluation

All the spoofs were identified as the original finger without exception and with high matching scores, as expected from the real ones. The quality of the images acquired and the scores reached in verification mode presented a good replication of the original finger. Finally, the false acceptance rate (FAR), the ability to deceive the system using the PAD, was higher than that of commercial materials, as reported hereafter.

The spoofs produced from the new materials showed a high rate of successful attacks on two of the three biometric systems, reaching high scores of deception, i.e., high FAR; the fakes which were prepared from commercially available polymers were rejected by the three systems at much higher rates, i.e., low FAR, as shown in Table 2.

The hydrogel spoofs (two batches, a and b) were accepted in about 80% and 60% of the trials on the first two devices (A and

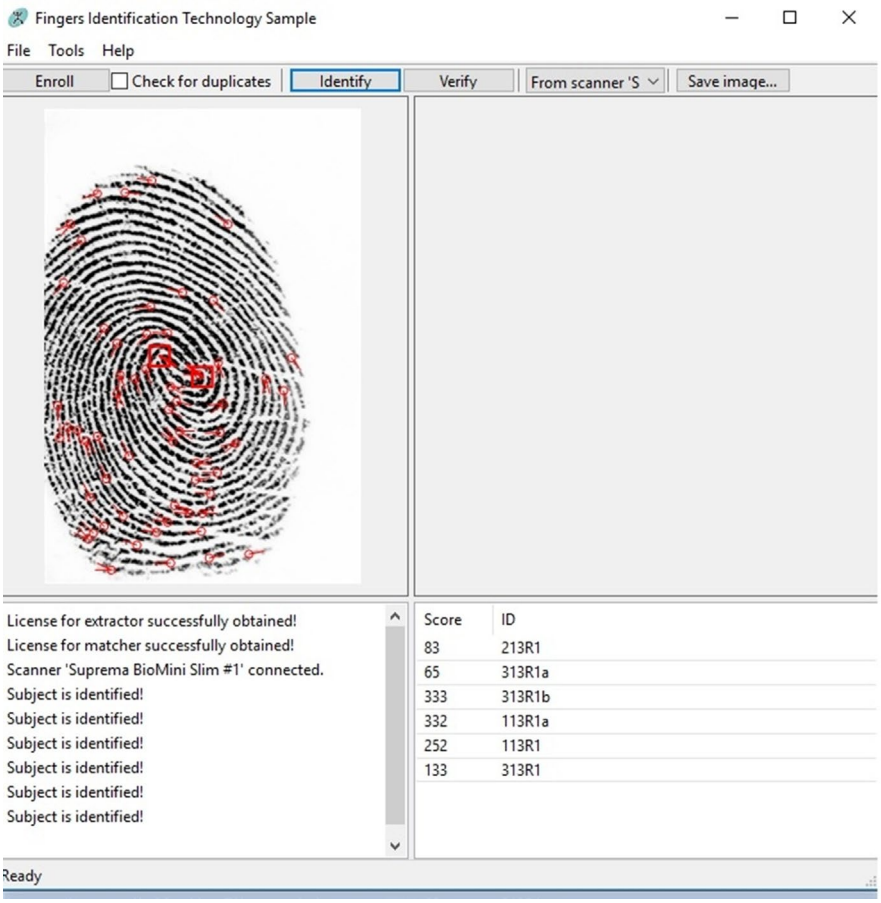

FIGURE 6 Example of a screen image of finger identification with Neurotec Biometric 6 – Identification score of hydrogel #2 spoof of subject no. 13 right index, enrolled with the reader no. 3

TABLE 2 False acceptance rates (FAR), materials versus readers

		A			B			C		
		Pass	Fail	%	Pass	Fail	%	Pass	Fail	%
Polyurethane		0	94	0	9	102	8.1	0	90	0
Silicone		6	88	6.4	6	105	5.4	0	108	0
Latex		80	19	80.8	1	92	1.1	0	96	0
Hydrogel #1	a	187	48	79.6	151	104	59.2	2	178	1.1
	b	160	35	82.0	103	74	58.2	0	61	0
Hydrogel #2	a	39	6	86.7	32	16	66.6	0	39	0
	b	34	1	97.1	32	8	80.0	0	17	0

B), respectively, while almost all the commercially available spoofs failed to fool these two systems, with the exception of the latex fakes versus the first one that accepted 80% of them.

All the spoofs were detected as such by the third device (C), based on multispectral technology, aside from the only two hydrogel-spoofs artifacts, which was probably a genuine error of the system.

3.2 | Software-based PAD

One *Spoof Detection software* was used as an example of presentation attack detection by image analysis. The false reject rate (FRR) of authentic fingers was about 21%, perceived as 79% acceptance rate, and is considered a relatively high error rate. The different spoofs attained a comparatively high FAR as well, as shown in Table 3, about 35% of the polyurethanes, 32% of the silicones, 18% of the latex, and 37% to 46% of the new polymers were falsely accepted.

3.3 | Image quality

The image quality attained by the different spoofs was measured by the NFIQ 2 image-analysis software, and compared with images of authentic fingers. The common practice is to accept the

TABLE 3 Acceptance and reject rates of the software-based PAD

	Authentic		Polyurethane		Silicone		Latex		Hydrogel #1		Hydrogel #2	
	Count	%	Count	%	Count	%	Count	%	Count	%	Count	%
Pass (>499)	64	79.0	9	34.6	13	31.7	6	18.2	36	36.7	16	45.7
Fail (<500)	17	21.0	7	26.9	27	65.9	9	27.3	37	37.8	18	51.4
No response	0	0.0	10	38.5	1	2.4	18	54.5	25	25.5	1	2.9
Total	81	100.0	26	100.0	41	100.0	33	100.0	98	100.0	35	100.0

highest 40% of the scoring images for enrollment, and the highest 60% for verification purposes. Most of the images reached acceptable quality scores, above 60, as seen in Table 4. Only 67% of the authentic fingers obtained a score higher than 60 and 98% more than 40, while the polyurethane and silicone artifacts attained slightly lower scores and the latex ones performed better. Only 42%–55% of the hydrogels achieved a score of more than 60, probably due to many air bubbles entrapped in the product. This could be improved by further optimization of the production technique. Nevertheless, most of them received high scores upon biometric identification, as mentioned above. It is noteworthy that the latex-spoofs attained the highest scores, even higher than authentic fingers, due to the higher quality of the replication with fewer imperfections and apparently better wetting capability relatively to fingers, as some might be too dry for good visualization on the readers.

4 | DISCUSSION

The new PEG-based hydrogels show high potential as novel spoofing materials. The efficiency of the spoofs was achieved by the particular structure of the rationally designed polymers.

As expected, due to the flexible segments along the polymer backbone and the hydrophilicity of the linking groups, the polymer was fine-tuned according to the length of the basic chain, the nature of the linking bond, or both. These segments produced chemical linking to water molecules and modified the polymers' properties according to their frequency along the polymer chain. The flexibility and the hydrophilicity achieved enabled the artifacts to present high-quality images of the fake fingerprints with an adequate electrical conductivity similar to real fingers when needed, effectively deceiving some PAD systems. The hydrogels, thus, prepared exhibited superior mechanical and electrical properties.

The solvent-casting method enabled clear reproduction of the fine details of the fingerprint, attaining high-quality NFIQ2 scores, and proved to be suitable for the task. Some spoofs achieved higher scores than the original real fingers, most likely owing to the higher wetting capabilities of the materials relative to fingers, dry fingers in particular which often present low-quality images. Several products presented some shortcomings expressed in lower quality scores, due principally to the presence of air bubbles in the casted finger. Hence, the production technique was subsequently improved and could be further developed, essentially by choosing the appropriate mixture of solvents and the optimal material concentration. Sample images of spoof fingerprints are seen in Figure 7.

The images acquired by the various devices reached relatively high false-acceptance rates of the software-based PAD system, showing the importance of the quality of the artifacts, allowing a high probability of successful spoofing by the presented method and materials.

Most of the hydrogel spoofs were not detected by some of the PAD systems, reaching much higher deceiving scores than those made up from commercial materials. Nevertheless, some systems

TABLE 4 NFIQ 2 image quality score distribution of the different spoofs vs. authentic fingers [%]

NFIQ2 score	Authentic	PU	Si	Latex	Hydrogel #1	Hydrogel #2
Number of images	81	26	41	33	118	38
>60	66.7	50.0	70.7	93.9	42.4	55.3
40~60	31.3	38.5	17.1	3.1	38.1	26.3
<40	2.0	11.5	12.2	3.0	19.5	18.4

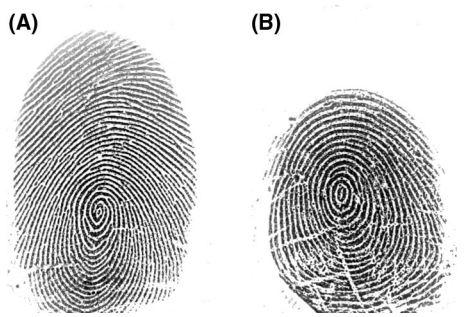

FIGURE 7 Images of hydrogel #1 (A) and hydrogel #2 (B) spoofs as acquired by device A. (optical)

are quite good at detecting spoofs; for example, the multispectral technology (device C) exhibited very good resistance to spoofing, even by the new materials. The use of different wavelengths allows scanning both surface and sub-surface features of the finger, efficiently distinguishing fakes from the reals. Similarly, the fourth reader, with a PAD system based on the electrical properties of the skin, rejected all the spoofs successfully.

5 | CONCLUSIONS

This research has illustrated the working concept of proactive forensic science in biometrics. This approach involves the exploitation of forensic science in order to generate new insights on crime, fingerprint spoofing in the present case. The threat of fingerprint spoofing is growing along with the increasing use of biometric systems and the constant race between crime and law enforcement agencies will most likely continue in this field due to the high possible gain for the criminals.

The aim of our work was to design new polymers with improved properties as potential fingerprint-spoofing materials. Flexible, hydrophilic materials with appropriate mechanical properties, which meet the functional requirements, have been developed by rationally modifying the polymers' structure.

New hydrogel-based spoofs were produced by gradually increasing the molecular weight of the basic polymer and changing the nature of the linking group, based on relatively simple and straight-forward chemistry. Several novel-material spoofs were manufactured and functionally tested, confirming the feasibility of conceiving such new materials able to effectively deceive some presentation attack detection systems. We showed that hydrogels are good candidates; hence, these new spoofing materials might present a serious threat to biometric readers and PAD systems.

Law enforcement agencies should be aware of this threat and take appropriate countermeasures, developing new technologies and methods to detect new sophisticated spoofs.

ORCID

Michel Saguy https://orcid.org/0000-0002-0738-4989
Joseph Almog https://orcid.org/0000-0002-1672-6477
Daniel Cohn https://orcid.org/0000-0002-4512-3632
Christophe Champod https://orcid.org/0000-0002-4035-2698

REFERENCES

1. Smolianitski E, Wolf E, Almog J. Proactive forensic science: a novel class of cathinone precursors. Forensic Sci Int. 2014;242:219–27. https://doi.org/10.1016/j.forsciint.2014.06.020.
2. Sabhanayagam T, Prasanna Venkatesan V, Senthamaraikannan K. A comprehensive survey on various biometric systems. Int J Appl Eng Res. 2018;13(5):2276–97.
3. Bhattacharyya D, Ranjan R, Alisherov FA, Choi M. Biometric authentication: a review. Int J Serv Sci Technol. 2009;2(3):13–28.
4. Mir A, Rubab S, Jhat Z. Biometrics verification: a literature survey. Int J Comput ICT Res. 2011;5(2):67–80.
5. Jain AK, Nandakumar K, Ross A. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognit Lett. 2016;79:80–105. https://doi.org/10.1016/j.patrec.2015.12.013.
6. Severance C. Anil Jain: 25 years of biometric recognition. Computer (Long Beach Calif). 2015;48(8):8–10. https://doi.org/10.1109/MC.2015.232.
7. Roy A, Memon N, Ross A. MasterPrint: exploring the vulnerability of partial fingerprint-based authentication systems. IEEE Trans Inf Forensics Secur. 2017;12(9):2013–25. https://doi.org/10.1109/TIFS.2017.2691658.
8. Matsumoto T, Matsumoto H, Yamada K, Hoshino S. Impact of artificial "gummy" fingers on fingerprint systems. In: van Renesse RL, editor. Proceedings of SPIE Optical Security and Counterfiet Deterrence Techniques IV; 2002 Jan 23-25; San Jose, CA. Bellingham, WA: SPIE; 2002. p. 275–89. doi: https://doi.org/10.1117/12.462719.
9. CCC: How to fake fingerprints? 2004. https://biometrics.mainguet.org/alive/site_archive/CCC_01_How_to_fake_fingerprints.htm. Accessed 11 Sept 2021.
10. Homeland Security News Wire. Japanese biometric border fooled by tape. 2010. http://www.homelandsecuritynewswire.com/japanese-biometric-border-fooled-tape. Accessed 15 June 2019.
11. The Sydney Morning Herald. Korean fools finger printing system. 2009. https://www.smh.com.au/world/korean-fools-finger-printing-system-20090101-78gk.html. Accessed 11 Sept 2021.
12. BBC Online. Doctor "used silicone fingers" to sign in for colleagues. 2013. https://www.bbc.com/news/world-latin-america-21756709. Accessed 15 June 2019.

13. BBC News. Kuwait cracks down on state employees faking work. 2017. https://www.bbc.com/news/blogs-news-from-elsewhere-39151942. Accessed 16 June 2019.
14. Rattani A, Scheirer WJ, Ross A. Open set fingerprint spoof detection across novel fabrication materials. IEEE Trans Inf Forensics Secur. 2015;10(11):2447–60. https://doi.org/10.1109/TIFS.2015.2464772.
15. Espinoza M, Champod C. Risk evaluation for spoofing against a sensor supplied with liveness detection. Forensic Sci Int. 2011;204(1–3):162–8. https://doi.org/10.1016/j.forsciint.2010.05.025.
16. Espinoza M, Champod C, Margot P. Vulnerabilities of fingerprint reader to fake fingerprints attacks. Forensic Sci Int. 2011;204(1–3):41–9. https://doi.org/10.1016/j.forsciint.2010.05.002.
17. Kanich O, Drahanský M, Mézl M. Use of creative materials for fingerprint spoofs. In: Proceedings of the 2018 International Workshop on Biometrics and Forensics (IWBF); 2018 June 6-7; Sassari, Italy. Piscataway, NJ: IEEE; 2018. doi: https://doi.org/10.1109/IWBF.2018.8401565.
18. Anusha MS, Kavitha KS. Fingerprint liveness detection analysis using hardware and software parameters to avoid spoofing. In: Proceedings of the 2017 International Conference on Electrical, Electronics, Communication Computer Technologies and Optimization Techniques (ICEECCOT); 2017 Dec 15-16; Mysuru, India. Piscataway, NJ: IEEE; 2018. p. 529–32.
19. Marcel S, Nixon MS, Li SZ, editors. Handbook of biometric anti-spoofing: Trusted biometrics under spoofing attacks. London, UK.: Springer; 2014.
20. HID Global. Biometrics – Multispectral technology comparison. 2015. https://www.hidglobal.com/sites/default/files/resource_files/hid-biometric-tech-comparison-ct-en.pdf. Accessed 16 May 2019.
21. Marasco E, Ross A. A survey on antispoofing schemes for fingerprint recognition systems. ACM Comput Surv. 2014;47(2):1–36. https://doi.org/10.1145/2617756.
22. Nixon KA, Aimale V, Rowe RK. Spoof detection schemes. In: Jain AK, Flynn P, Ross AA, editors. Handbook of biometrics. New York, NY: Springer; 2008. p. 403–23.
23. Galbally J, Marcel S, Fierrez J. Biometric antispoofing methods: a survey in face recognition. IEEE Access. 2014;2:1–23. https://doi.org/10.1109/ACCESS.2014.2381273.
24. Sandström M. Liveness detection in fingerprint recognition systems. Linköping, Sweden: Institutionen för Syst Univ Linköping; 2004.
25. BSI. Certification report: BSI-DSZ-CC-0790-2013 for MorphoSmart Optic 301, Version 1.0, from Safran Morpho. Bonn, Germany: Federal Office for Information Security; 2013.
26. Kumar M. An overview of live detection techniques to secure fingerprint recognition system from spoofing attacks. London J Res Comput Sci Technol. 2018;18(1):23–31.
27. Yuan C, Li X, Wu QMJ, Li J, Sun X. Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. Comput Mater Contin. 2017;53(4):357–72. https://doi.org/10.3970/cmc.2017.053.357.
28. Kim W. Towards real biometrics: An overview of fingerprint liveness detection. In: Proceedings of the 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA); 2016 Dec 13-16; Jeju, Korea. Piscataway, NJ: IEEE, 2016. p. 1–3. https://doi.org/10.1109/APSIPA.2016.7820888.
29. Sousedik C, Busch C. Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biometrics. 2014;3(4):219–33. https://doi.org/10.1049/iet-bmt.2013.0020.
30. Javelin Strategy. Identity fraud hits all time high with 16.7 million U.S. victims in 2017, according to new Javelin Strategy & Research study. 2018. https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin. Accessed 16 June 2019.
31. Sanderson TM. Transnational terror and organized crime: blurring the lines. SAIS Rev. 2004;24(1):49–61. https://doi.org/10.1353/sais.2004.0020.
32. Willox NA, Regan TM. Identity fraud: providing a solution. J Econ Crime Manag. 2002;1(1):1–15.
33. Bjelopera JP, Finklea KM. Organized crime: an evolving challenge for U.S. law enforcement. Congressional research service. 2013. https://crsreports.congress.gov/product/pdf/R/R41547. Accessed 3 March 2020.
34. Jackson BA. Technology acquisition by terrorist groups: Threat assessment informed by lessons from private sector technology adoption. Stud Confl Terror. 2001;24(3):183–213. https://doi.org/10.1080/10576100151130270.
35. Martinu O, McEwen G. Crime in the age of technology. Eur Law Enforc Res Bull. 2018;(4 SCE):23–8.
36. Almog J. Forensics as a proactive science. Sci Justice. 2014;54(5):325–6. https://doi.org/10.1016/j.scijus.2014.05.008.
37. Irons A, Lallie H. Digital forensics to intelligent forensics. Futur Internet. 2014;6(3):584–96. https://doi.org/10.3390/fi6030584.
38. Carlsson A, Lindberg S, Wu X, Dunne S, Josefsson M, Astot C, et al. Prediction of designer drugs: Synthesis and spectroscopic analysis of synthetic cannabinoid analogues of 1H-indol-3-yl(2,2,3,3-tetramethylcyclopropyl) methanone and 1H-indol-3-yl(adamantan-1-yl)methanone. Drug Test Anal. 2016;8(10):1015–29. https://doi.org/10.1002/dta.1904.
39. Hoffman AS. Hydrogels for biomedical applications. Adv Drug Deliv Rev. 2012;64:18–23. https://doi.org/10.1016/j.addr.2012.09.010.
40. Schacht EH. Polymer chemistry and hydrogel systems. J Phys Conf Ser - IOP Publishing. 2004;3:22–8. https://doi.org/10.1088/1742-6596/3/1/004.
41. Cohn D, Sosnik A, Garty S. Smart hydrogels for in situ generated implants. Biomacromolecules. 2005;6(3):1168–75. https://doi.org/10.1021/bm0495250.
42. Gibas I, Janik H. Review: synthetic polymer hydrogels for biomedical applications. Chem Chem Technol. 2010;4(4):297–304. https://doi.org/10.23939/chcht04.04.297.
43. Champod C, Espinoza M. Forgeries of fingerprints in forensic science. In: Marcel S, Nixon MS, Li SZ, editors. Handbook of biometric anti-spoofing. London, UK: Springer; 2014. p. 13–34.
44. Marcialis GL, Lewicke A, Tan B, Coli P, Grimberg D, Congiu A, et al. First international fingerprint liveness detection competition – LivDet 2009. In: Foggia P, Sansone C, Vento M, editors. Image analysis and processing – ICIAP 2009. Berlin/Heidelberg, Germany: Springer Berlin Heidelberg; 2009. p. 12–23.
45. Ghiani L, Yambay D, Mura V, Tocco S, Marcialis GL, Roli F, et al. LivDet 2013 –Fingerprint liveness detection competition 2013. In: Proceedings of the 6th IAPR International Conference on Biometrics (ICB); 2013 June 4-7; Madrid, Spain. Piscataway, NJ: IEEE; 2013. p. 1–6.
46. Yambay D, Ghiani L, Denti P, Marcialis GL, Roli F, Schuckers S. LivDet 2011 – Fingerprint liveness detection competition 2011. In: Proceedings of the 5th IAPR International Conference on Biometrics (ICB); March 29 - April 1; New Delhi, India. Piscataway, NJ: IEEE; 2012. p. 208–15.
47. Ghiani L, Yambay DA, Mura V, Marcialis GL, Roli F, Schuckers SA. Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015. Image Vis Comput. 2017;58:110–28. https://doi.org/10.1016/j.imavis.2016.07.002.
48. Mura V, Orru G, Casula R, Sibiriu A, Loi G, Tuveri P, et al. LivDet 2017 – Fingerprint liveness detection competition 2017. Proceedings of the 2018 IAPR International Conference on Biometrics (ICB); 2018

Feb 20-23; Gold Coast, Queensland. Piscataway, NJ: IEEE; 2018. p. 297–302.
49. National Institute of Standards and Technology (NIST). Biometric quality homepage. 2019. https://www.nist.gov/programs-projects/biometric-quality-homepage. Accessed 1 Feb 2020.
50. NIST. Development of NFIQ 2.0. 2018. https://www.nist.gov/services-resources/software/development-nfiq-20. Accessed 19 Dec 2019.

How to cite this article: Saguy M, Almog J, Cohn D, Champod C. Proactive forensic science in biometrics: Novel materials for fingerprint spoofing. J Forensic Sci. 2021;00:1–9. https://doi.org/10.1111/1556-4029.14908