5-16-2019

Inkjet-Printed Carbon Nanotubes for Fabricating a Spoof Fingerprint on Paper.

Veasna Soum
Sogang University

Sooyoung Park
Sogang University

Albertus Ivan Brilian
Sogang University

Yunpyo Kim
Sogang University

Madeline Y Ryu
United States Military Academy

See next page for additional authors

Recommended Citation

Soum, V., Park, S., Brilian, A. I., Kim, Y., Ryu, M. Y., Brazell, T., ... & Shin, K. (2019). Inkjet-printed carbon nanotubes for fabricating a spoof fingerprint on paper. ACS omega, 4(5), 8626-8631. https://doi.org/10.1021/acsomega.9b00936

ACS OMEGA

Article

Cite This: ACS Omega 2019, 4, 8626−8631

http://pubs.acs.org/journal/acsodf

Inkjet-Printed Carbon Nanotubes for Fabricating a Spoof Fingerprint on Paper

Veasna Soum,[†] Sooyoung Park,[†] Albertus Ivan Brilian,[†] Yunpyo Kim,[†] Madeline Y. Ryu,[‡] Taler Brazell,[‡] F. John Burpo,[‡] Kevin Kit Parker,[§,⊥] Oh-Sun Kwon,[†] and Kwanwoo Shin*[,†]

[†]Department of Chemistry, Institute of Biological Interfaces, Sogang University, Seoul 04107, Republic of Korea

[‡]Department of Chemistry and Life Science, United States Military Academy, West Point, New York 10996, United States

[§]John A. Paulson School of Engineering and Applied Sciences, Harvard University, Cambridge, Massachusetts 02138, United States

[⊥]Department of Chemistry and Life Science, United States Military Academy, West Point, New York 10996, United States

Supporting Information

ABSTRACT: A spoof fingerprint was fabricated on paper and applied for a spoofing attack to unlock a smartphone on which a capacitive array of sensors had been embedded with a fingerprint recognition algorithm. Using an inkjet printer with an ink made of carbon nanotubes (CNTs), we printed a spoof fingerprint having an electrical and geometric pattern of ridges and furrows comparable to that of the real fingerprint. With this printed spoof fingerprint, we were able to unlock a smartphone successfully; this was due to the good quality of the printed CNT material, which provided electrical conductivities and structural patterns similar to those of the real fingerprint. This result confirms that inkjet-printing CNTs to fabricate a spoof fingerprint on paper is an easy, simple spoofing route from the real fingerprint and suggests a new method for outputting the physical ridges and furrows on a two-dimensional plane.

INTRODUCTION

Since the 1980s, inkjet printers became the most commonly used type of printers. However, inkjet printing using the diverse materials as ink is a relatively new technology, providing a great opportunity for various applications such as electronic circuits,[1] batteries,[2] semiconductors,[3] optical devices,[4,5] microfluidics,[6−9] and sensors.[10−13] Inkjet printing allows a specific design to be printed with high resolution in a simple, fast, low-cost process and with low material waste.[14−17] Carbon nanotubes (CNTs) are common materials used for printing conductive circuits and sensors because they have good electrical conductivity, high surface sensing area, and high stability and because they can be dispersed in a typical solvent.[15,18−23] Kwon et al. successfully formulated CNT ink for inkjet printing and used the ink for printing simple conductive electrodes and digital microfluidic chips on paper.[6,7,24]

Physiological biometric traits, such as the characteristics of one's face, iris, hand, finger-vein, and fingerprints, are unique to an individual.[25,26] Fingerprints have routinely been used for personal identification since their first use by a French police expert, A. Bertillon, in the 19th century; they have also been used in China as signatures on legal documents for 3000 years.[27−29] The fingerprint has become a highly secure biometric key for accessing personal and financial information on smartphones equipped with cutting-edge security features, including a fingerprint sensor and appropriate software.

A possible way to attack such a fingerprint sensor device is to generate a spoof fingerprint from its owner's latent fingerprint.[30,31] Spoof fingerprints can be made using a molding method or an inkjet printing method.[30−34] In 2016, Cao reported an easy and simple spoofing attack to unlock the home button (unlock button) of smartphones by using a spoof fingerprint that had been fabricated with silver ink through inkjet printing.[31]

Herein, we report the results of our research in which we investigated a novel CNT ink that would allow a simpler, more easily accessible way to fabricate a spoof fingerprint by using an inkjet printer. Furthermore, the CNT-printed patterns have better flexibility and stability in ambient conditions compared to metal-based ones, in addition to the ease of use and economical advantages. We described in detail about characterizations of the printed CNT patterns versus printing conditions and image processing on an image of a latent fingerprint in order to create a good spoof fingerprint. Finally, we used the printed spoof fingerprint to attack successfully a smartphone with a fingerprint sensor device (Figure 1).

RESULTS AND DISCUSSION

Inkjet-Printed CNT Ink on Paper. A CNT has a cylindrical tube structure seamlessly rolled by using a graphene sheet, which is a hexagonal lattice of carbon atoms. It has uniquely superior mechanical, electrical, optical, and thermal properties that

Received: April 3, 2019
Accepted: May 7, 2019
Published: May 16, 2019

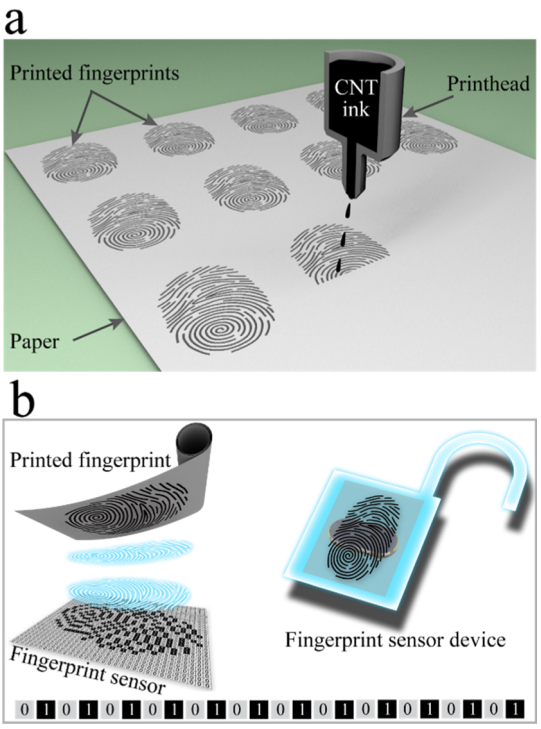

Figure 1. Schematic illustrations: (a) printing of spoof fingerprints on paper and (b) spoofing attack using the printed fingerprint on a representative fingerprint sensor device.

depend on its characteristics, such as its length, diameter, rolling-up geometry as well as the presence of functional ligands.[35,36] The diameter and length of a CNT were measured by using ImageJ software in a scanning electron microscopy (SEM) image in Figure 2b. The results showed that the average

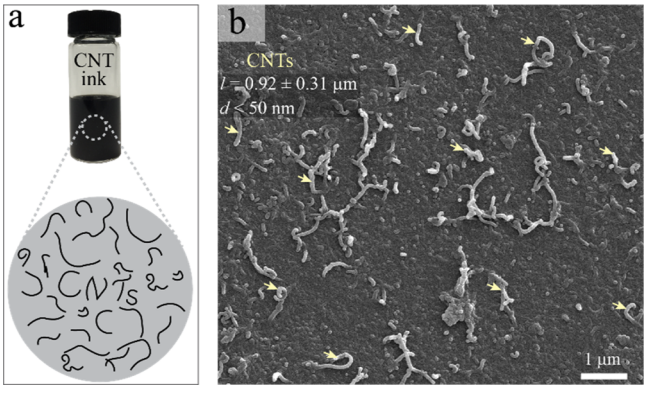

Figure 2. (a) Dispersed CNT ink for inkjet printing and (b) SEM image of CNTs, showing their lengths (l) and diameters (d).

diameter and length of the CNT were about $d < 50$ nm and $l = 0.92 \pm 0.31$ μm, respectively. The average length of the CNT is one-twentieth of the 21 μm nozzle diameter, allowing the inkjet printer to jet out the CNT ink without clogging.[15,31] Using the fluidic parameters of our CNT ink, that is, a viscosity of ~2 cP and a surface tension of ~40 mN/m, we determined that the jetting condition of the inkjet printer was satisfied (Video Clip S1).[24,37]

By using our prepared CNT ink with its optimized properties, we printed on paper CNT patterns with a fingerprint-like design (Figure 3a). The printed pattern showed a clean edge that

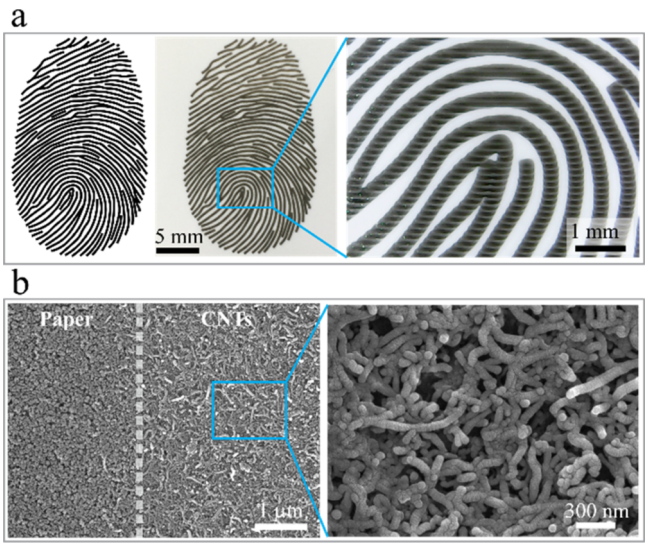

Figure 3. (a) Mimic design of fingerprint patterns and a printed image of the CNT pattern. (b) SEM image showing the surface morphologies of the CNT pattern/printing paper (left) and high-magnification SEM image of the CNTs (right).

resulted from the optimum properties of the ink, the inkjet printer, and the printing paper, which had a glossy surface. After we had printed the design with CNT ink, we investigated its morphology by using SEM. The SEM image showed the presence of CNTs in the printed pattern aggregated on the glossy surface of the paper (Figure 3b). That aggregation of CNTs provided physical contact that allowed the printed CNT pattern to conduct electricity. The printed CNT patterns showed no hint of conductivity breakdown even after the bend cycles for 500 times at a bend angle of 180°.

An error in the printing of an aqueous ink by using the inkjet printing method commonly causes the printed drop placement to be inaccurate by about ±3 μm with a 300 μm throw distance, which is the distance from the printhead to the printing substrate[38] and a spreading of the printed drop on the printing substrate through the wettability phenomena.[39,40] These factors can make a printed pattern larger than its actual design. To observe changes in the area of the patterns printed using our setup, we designed a pattern with a total area of 1 mm^2 (l = 5 mm, w = 0.2 mm) and printed it from 1 to 10 times (Figure 4a inset). After the CNT patterns had been printed, we measured the total area of the patterns by using ImageJ software. Data showed that the total area of the printed pattern was larger than the actual design by about 0.35 mm^2 for one printing, increased to about 0.60 mm^2 for two printings, and continued to increase slightly after the second printing (Figure 4a). Figure 4b shows the surface profiles of the CNT-printed patterns; the height is seen to increase approximately from 0.3 to 1.7 μm as the number of printings was increased from 1 to 10.

Because the electrical conductivity of a CNT pattern depends on the printed CNT network, the conductivity of a CNT pattern can be improved by increasing the number of printings. To investigate the electrical conductivity of the CNT-printed patterns, we measured the surface sheet resistance of a CNT electrode printed on paper as a function of the number of printings. Figure 4c shows that the surface sheet resistance of the printed CNT pattern is roughly 3.4 kΩ/sq for one printing, decreases to about 0.6 kΩ/sq for five printings, and continues to decrease slightly to 0.4 kΩ/sq as more printings are added.

DOI: 10.1021/acsomega.9b00936
ACS Omega 2019, 4, 8626−8631

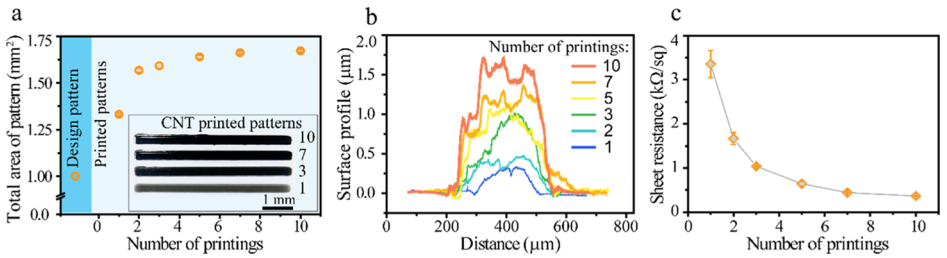

Figure 4. Properties of printed CNT patterns as a function of printings: (a) total area of the printed patterns, (b) surface profiles, and (c) electrical surface sheet resistance vs number of printings.

Image Processing for a Spoof Fingerprint. In addition to providing electrical similarity, in order to prepare a spoof fingerprint, we performed an image transformation from the real fingerprint to the fake fingerprint in four steps (Figure 3): capture, electronic transformation, image processing, and printing.

Capture: Collecting a fingerprint would be very complicated, complex forensic process if we tried to get it non-noticeably or illegally from its owner without permission, for example, by taking surreptitiously the fingerprint left on the smartphone's screen. In this study, we skipped this spoofing step by directly copying the real fingerprint of the right index finger in black stamp ink onto printing photo paper with a white background. In the capture step, the tip of the finger was cleaned with alcohol, covered with ink evenly, dried for about 30−60 s, and pressed slightly so that the fingerprint was copied in ink onto the photo paper. A precise copy of the patterns from the original fingerprint was achieved by allowing the ink on the fingerprint to dry before transferring it and using photo paper as a substrate.

Electronic Transformation (Figure 5a): We used an office scanner for capturing a fingerprint image with a scanning

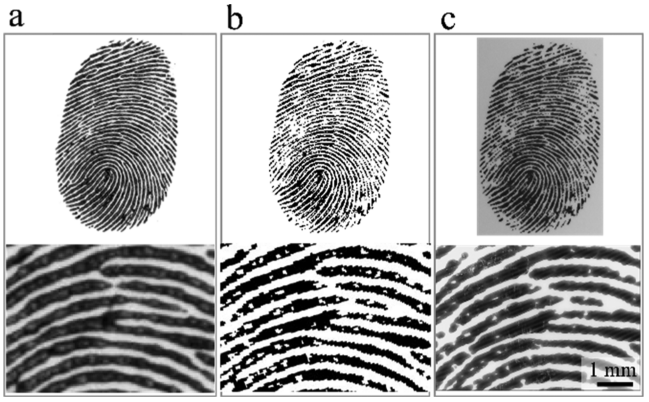

Figure 5. Imaging process for generating a copy of a fingerprint by printing. Fingerprint images obtained after (a) scanning and flipping horizontally and (b) adjusting the contrast. (c) Higher-magnification image of the printed fingerprint.

resolution of 500 dpi. The image should be scanned in the range of 300 dpi or higher resolution. The images scanned with different resolutions should be processed (contrast adjustment) in the image processing step differently in order to obtain desired fingerprint image.

Image Processing (Figure 5b): Using ImageJ software, we modified the scanned image to obtain a good-quality fingerprint. Initially, the scanned image was processed with the threshold option to adjust the contrast of the image (contrast = 215) and to erase the blur, which had been created mostly during the image capture and scanning steps. We also used the threshold option to optimize the dimension of the printing ridge patterns in order to generate an identically printed fingerprint. Because the captured image was a mirror image of the real one, it was transformed into the flip-horizontal image that was needed for the fake image for our spoofing attack.

Printing (Figure 5c): We used an inkjet printer with CNT ink to pattern the fingerprint images on photo paper. To obtain good-quality printed patterns, we set our printing condition to six printing nozzles, a 20 μm drop spacing, and a 1270 dpi printing resolution.

Printed CNT Pattern as a Spoof Fingerprint. A fingerprint is composed of a series of friction ridges (500−700 μm in width and 40−60 μm in height) and furrows on the epidermis of the skin of the human finger.[33,41,42] The uniqueness of a fingerprint is due to its overall pattern of friction ridges and its minutiae, such as ending ridges, deltas, bifurcations, dots, and lakes; moreover, a fingerprint does not change and is specific to the individual such that it has used for personal identification.[28,29,41] In addition to its specific structures and shapes, a fingerprint has an electrical property, that is, a resistance of about 2 kΩ to 2 MΩ.[43,44]

In order to generate a spoof fingerprint that has characteristics similar to those of a real fingerprint, we printed a latent fingerprint pattern by using an inkjet printer with conductive CNT ink. With the printing setup, we could print spoof fingerprint patterns that not only mimicked the shapes of fingerprint patterns but were also electrically conductive. Before the printing, we optimized the latent fingerprint, as mentioned in the image processing section. We printed the latent fingerprint various numbers of times to select the best printing condition for generating a printed fingerprint identical to the latent fingerprint. Figure 6a shows that the total area of the printed fingerprint was larger than the total area of the processed image by approximately 18 mm^2 for one printing. Moreover, the total area of the printed fingerprint was smaller than that of the original latent fingerprint by roughly 18 mm^2. The spoof fingerprint fabricated using two printings had a total area larger than that of the original latent fingerprint by approximately 18 mm^2. Thus, one and two printings provided total areas similar to that of the original latent fingerprint. The data also showed that the total area of printed fingerprint pattern dramatically increased with increasing number of printings.

To observe the changes in the widths of the ridges and the furrows of the printed fingerprint, we selected three ridges and furrows and then measured the changes in their widths. We found that the width of the ridge printed 10 times was about 40 μm larger than the width of the ridge printed one time, whereas the furrow width of the printed fingerprint decreased with increasing number of printings (Figure 6b). One and two printings provided patterns similar to those of the latent

DOI: 10.1021/acsomega.9b00936
ACS Omega 2019, 4, 8626−8631

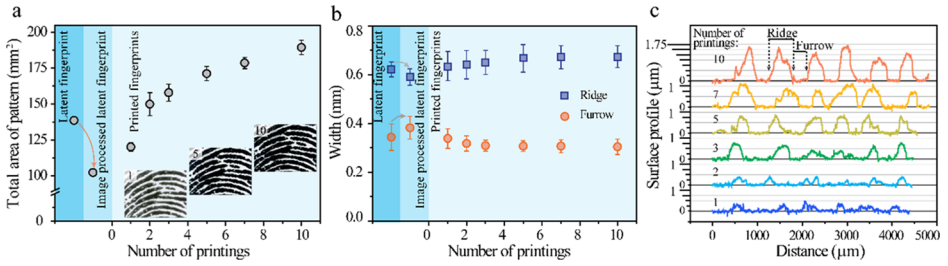

Figure 6. Characterization of the printed fingerprint: (a) total area of the printed fingerprint pattern vs the number of printings, (b) widths of a ridge and a furrow of the printed fingerprint pattern vs the number of printings, and (c) surface profiles of the ridges and the furrows of the printed fingerprint for various numbers of printings.

fingerprint. We measured the surface profiles of the printed fingerprints across six ridges and five furrows (Figure 6c). The physical structure (height) of the printed fingerprint increased with increasing number of printings, which made the printed ridges more distinguishable.

Spoofing Attack on a Fingerprint Capacitive Sensor. A fingerprint can be used as an identification key via a fingerprint sensor embedded in the unlock button and in the recognition system of a smartphone. According to Galbally et al., who compared the detected fingerprint with the stored one, identification was verified and access was authorized if at least a dozen characteristics and minutiae among the extracted features of the fingerprint used for entry matched those of the fingerprint in storage.[45]

The capacitive sensor works by detecting changes in capacitance across its electronic circuits under the influence of a conductor on its surfaces. The capacitance of a parallel plate capacitance, C, is

$$C = \kappa\varepsilon_0 \frac{A}{d} \tag{1}$$

where κ, ε_0, and A and d are the dielectric constant, the permittivity of free space, and the area of and the distance between the plates, respectively. The top plate of the capacitive sensor was replaced by a patterned CNT electrode printed on paper, thus forming an electrically equivalent sensing capacitor, C_s (the capacitor in Figure 7, colored in orange),[46,47] and ground capacitor, C_b (the capacitor in Figure 7, colored in green). Because the CNT plate was charged with free electrons at the moment of touching, at least the sensor's capacitance was clearly detected, along with a specific relatively small additive perturbation that was caused by the long, conductive-CNT-ridge electrode acting as a grounding plate. As a result, our ungrounded fake fingerprint was detectable (Figure 7).

Once the latent fingerprints had been printed from 1 to 10 times, individually printed fingerprints were cut out by using scissors. We used each printed fingerprint for a spoofing attack on the unlock button of a smartphone, Samsung Galaxy A5, which had been preprogrammed with the owner's real fingerprint. It should be noted that many trials were needed to exert the pressure of the printed pattern on the unlock button, which must be similar to that usually exerted by the owner. After the spoofing attack on the phone, we found that the fingerprints printed one, two, three, and five times had been successful in unlocking the phone (Figure 7, Video Clip S2), whereas the fingerprints printed more than five times failed to unlock the phone. This is because the fingerprints printed one, two, three, and five times generated ridges that were identical in width to the original latent fingerprint, while the others had much larger

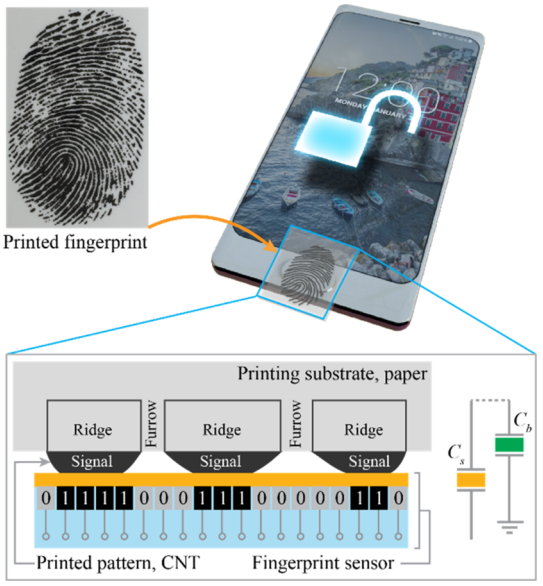

Figure 7. Spoofing attack to unlock a smartphone by using a printed paper-based fingerprint and mechanism through which a printed paper-based fingerprint sends the electronic signals necessary to unlock the fingerprint sensor.

widths. We also discovered that the spoofing attack typically invoked two types of responses: the phone was unlocked instantaneously on the first try or in less than 10 trials in about a minute for the case of using the spoof fingerprints printed two and three times, and the phone was unlocked after many attempts, which took as long as 20 min for the case of using the spoof fingerprint printed one and five times. We believe that the cause of difference in responses was not only contributed from the exactness in width to the original latent fingerprint but also caused by the thickness of the printed patterns.

CONCLUSIONS

We made a fingerprint by using an inkjet printer to print CNT ink on paper and successfully applied that fingerprint for a spoofing attack to unlock the start button of a smartphone. Because of the unique features of the CNT ink over other conducting metal-based inks, this method had the advantage of being easily accessible, without the need for a posttreatment. We demonstrated that by mimicking real ridges that were CNT-printed electrodes, a conductive CNT ink could be used to unlock a currently available smartphone. We emphasize that current security systems, without reinforced protection, may not be able to prevent a spoofing attack using a printed spoof fingerprint from being successful. If spoofing attacks on

DOI: 10.1021/acsomega.9b00936
ACS Omega 2019, 4, 8626−8631

biometric devices are to be avoided, users must be careful not to leave latent fingerprints on any devices, digital images, or places.

EXPERIMENTAL DETAILS

In this experiment, an aqueous printable ink made of multiwalled CNTs was used with a nonpolar organic dispersant, as described in our previous report.[24] After being mixed and dispersed, CNTs were filtered with a 1 μm pore filter (GF/B, Whatman) to be used with an inkjet printer (Figure 2a). The ink's surface tension and viscosity were measured by using a surface tension analyzer (SmartDrop, Femtobiomed) and a rheometer (Brookfield, RVDV-III Ultra), respectively. An ink cartridge (DMC-11610, Fujifilm, USA) was filled with the CNT ink, and an inkjet printer (Dimatix, DMP-2831, Fujifilm, USA) was used for the printing. A scanner (XP-225, Epson) was used to scan the fingerprint, which had been captured by pressing the real fingerprint covered with black stamp ink (Mae-Pyo) on photo paper (HB4020). We used the inkjet printer with the CNT ink to create a spoof fingerprint on the same photo paper (HB4020). The surface roughness (R_a) and surface contact angle of the photo paper were approximately 10 nm and 40°, respectively. The image processing and analyzing were carried out by using a freeware program (ImageJ).

The surface properties of the printed patterns were analyzed using a surface profiler (Dektak-XT, Bruker). A USB microscope (U500X, Cooling Tech) and a scanning electron microscope (JSM-6710F, JEOL) were employed for image analysis. A four-point measurement of the surface resistance was carried out by using Lucas Pro4 with a Keithley 2400 source meter (Keithley Instruments).

ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge on the ACS Publications website at DOI: 10.1021/acsomega.9b00936.

Inkjet printing of the CNT ink: focusing on drop jetting from the printing nozzles (AVI)

Unlock a smartphone with the printed spoof fingerprint (AVI)

AUTHOR INFORMATION

Corresponding Author

*E-mail: kwshin@sogang.ac.kr.

ORCID

Veasna Soum: 0000-0003-4164-2379

Kevin Kit Parker: 0000-0002-5968-7535

Kwanwoo Shin: 0000-0002-7563-8581

Notes

The authors declare no competing financial interest.

ACKNOWLEDGMENTS

The authors gratefully acknowledge financial support from the Basic Science Research Program (2017R1D1A1B03032095 and 2018R1A6A1A03024940) and the Leading Foreign Institute Recruitment Program (2013K1A4A3055268) through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology, and from the Grant Program (20174010201150) funded by the Ministry of Trade, Industry & Energy, Korea. O.-S.K. and K.S. acknowledge financial support from the Seoul R&BN Program (CU15006) funded by the Seoul Metropolitan City. T.B., M.Y.R., and F.J.B. acknowledge financial support from the 2016 US Military Academy-Academic Individual Advanced Development (AIAD) program.

REFERENCES

(1) Wang, Y.; Guo, H.; Chen, J.-j.; Sowade, E.; Wang, Y.; Liang, K.; Marcus, K.; Baumann, R. R.; Feng, Z.-s. Paper-Based Inkjet-Printed Flexible Electronic Circuits. *ACS Appl. Mater. Interfaces* **2016**, *8*, 26112−26118.

(2) Choi, K.-H.; Yoo, J.; Lee, C. K.; Lee, S.-Y. All-inkjet-printed, solid-state flexible supercapacitors on paper. *Energy Environ. Sci.* **2016**, *9*, 2812−2821.

(3) Kim, S.; Ko, H.; Lee, C.; Kim, M.; Kim, K. S.; Lee, Y.-H.; Shin, K.; Cho, Y.-H. Semiconductor Photonic Nanocavity on a Paper Substrate. *Adv. Mater.* **2016**, *28*, 9765−9769.

(4) Hou, J.; Li, M.; Song, Y. Patterned Colloidal Photonic Crystals. *Angew. Chem., Int. Ed.* **2018**, *57*, 2544−2553.

(5) Wu, L.; Dong, Z.; Li, F.; Zhou, H.; Song, Y. Emerging Progress of Inkjet Technology in Printing Optical Materials. *Adv. Opt. Mater.* **2016**, *4*, 1915−1932.

(6) Ruecha, N.; Lee, J.; Chae, H.; Cheong, H.; Soum, V.; Preechakasedkit, P.; Chailapakul, O.; Tanev, G.; Madsen, J.; Rodthongkum, N.; Kwon, O.-S.; Shin, K. Paper-Based Digital Microfluidic Chip for Multiple Electrochemical Assay Operated by a Wireless Portable Control System. *Adv. Mater. Technol.* **2017**, *2*, 1600267.

(7) Ko, H.; Lee, J.; Kim, Y.; Lee, B.; Jung, C.-H.; Choi, J.-H.; Kwon, O.-S.; Shin, K. Active Digital Microfluidic Paper Chips with Inkjet-Printed Patterned Electrodes. *Adv. Mater.* **2014**, *26*, 2335−2340.

(8) Fobel, R.; Kirby, A. E.; Ng, A. H. C.; Farnood, R. R.; Wheeler, A. R. Paper microfluidics goes digital. *Adv. Mater.* **2014**, *26*, 2838−2843.

(9) Yamada, K.; Henares, T. G.; Suzuki, K.; Citterio, D. Paper-Based Inkjet-Printed Microfluidic Analytical Devices. *Angew. Chem., Int. Ed.* **2015**, *54*, 5294−5310.

(10) Bihar, E.; Wustoni, S.; Pappa, A. M.; Salama, K. N.; Baran, D.; Inal, S. A fully inkjet-printed disposable glucose sensor on paper. *npj Flex. Electron.* **2018**, *2*, 30.

(11) Ruecha, N.; Chailapakul, O.; Suzuki, K.; Citterio, D. Fully Inkjet-Printed Paper-Based Potentiometric Ion-Sensing Devices. *Anal. Chem.* **2017**, *89*, 10608−10616.

(12) Bali, C.; Brandlmaier, A.; Ganster, A.; Raab, O.; Zapf, J.; Hübler, A. Fully Inkjet-Printed Flexible Temperature Sensors Based on Carbon and PEDOT:PSS1. *Mater. Today: Proc.* **2016**, *3*, 739−745.

(13) Chae, H.; Jung, M.; Cheong, H.; Soum, V.; Jo, S.; Kim, H.; Kim, T.; Kim, K.; Jeon, S.; Kwon, O. S.; Shin, K. Thermoelectric temperature sensors by printing with a simple office inkjet printer. *TechConnect Briefs* **2016**, *4*, 151−155.

(14) Raut, N. C.; Al-Shamery, K. Inkjet printing metals on flexible materials for plastic and paper electronics. *J. Mater. Chem. C* **2018**, *6*, 1618−1641.

(15) Andò, B.; Baglio, S.; Bulsara, A.; Emery, T.; Marletta, V.; Pistorio, A. Low-Cost Inkjet Printing Technology for the Rapid Prototyping of Transducers. *Sensors* **2017**, *17*, 748.

(16) Tao, R.; Ning, H.; Chen, J.; Zou, J.; Fang, Z.; Yang, C.; Zhou, Y.; Zhang, J.; Yao, R.; Peng, J. Inkjet Printed Electrodes in Thin Film Transistors. *IEEE J. Electron Devices Soc.* **2018**, *6*, 774−790.

(17) Andò, B.; Baglio, S.; Bulsara, R. A.; Emery, T.; Marletta, V.; Pistorio, A. Low-Cost Inkjet Printing Technology for the Rapid Prototyping of Transducers. *Sensors* **2017**, *17*, 748.

(18) Zaporotskova, I. V.; Boroznina, N. P.; Parkhomenko, Y. N.; Kozhitov, L. V. Carbon nanotubes: Sensor properties. A review. *Mod. Electron. Mater.* **2016**, *2*, 95−105.

(19) Tortorich, R.; Choi, J.-W. Inkjet Printing of Carbon Nanotubes. *Nanomaterials* **2013**, *3*, 453−468.

(20) Kholghi Eshkalak, S.; Chinnappan, A.; Jayathilaka, W. A. D. M.; Khatibzadeh, M.; Kowsari, E.; Ramakrishna, S. A review on inkjet printing of CNT composites for smart applications. *Appl. Mater. Today* **2017**, *9*, 372−386.

DOI: 10.1021/acsomega.9b00936
ACS Omega 2019, 4, 8626−8631

(21) Liao, W.-H.; Tien, H.-W.; Hsiao, S.-T.; Li, S.-M.; Wang, Y.-S.; Huang, Y.-L.; Yang, S.-Y.; Ma, C.-C. M.; Wu, Y.-F. Effects of multiwalled carbon nanotubes functionalization on the morphology and mechanical and thermal properties of carbon fiber/vinyl ester composites. *ACS Appl. Mater. Interfaces* **2013**, *5*, 3975−3982.
(22) Bandaru, P. R. Electrical properties and applications of carbon nanotube structures. *J. Nanosci. Nanotechnol.* **2007**, *7*, 1239−1267.
(23) Soum, V.; Cheong, H.; Kim, K.; Kim, Y.; Chuong, M.; Ryu, S. R.; Yuen, P. K.; Kwon, O.-S.; Shin, K. Programmable Contact Printing Using Ballpoint Pens with a Digital Plotter for Patterning Electrodes on Paper. *ACS Omega* **2018**, *3*, 16866−16873.
(24) Kwon, O.-S.; Kim, H.; Ko, H.; Lee, J.; Lee, B.; Jung, C.-H.; Choi, J.-H.; Shin, K. Fabrication and characterization of inkjet-printed carbon nanotube electrode patterns on paper. *Carbon* **2013**, *58*, 116−127.
(25) Rinaldi, A. Biometrics' new identity–measuring more physical and biological traits: Research into the characteristics that are unique to an individual is addressing the need to correctly identify people in a variety of medical, social and security contexts. *EMBO Rep.* **2016**, *17*, 22−26.
(26) Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Chaudhry, J.; Adi, E.; Valli, C. Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem. *IEEE Access* **2018**, *6*, 36939−36947.
(27) Jain, A. K. Technology: biometric recognition. *Nature* **2007**, *449*, 38−40.
(28) Qinghai, G. A Preliminary Study of Fake Fingerprints. *Int. J. Comput. Netw. Inf. Secur.* **2014**, *6*, 1−8.
(29) Unar, J. A.; Seng, W. C.; Abbasi, A. A review of biometric technology along with trends and prospects. *Pattern Recognit.* **2014**, *47*, 2673−2688.
(30) Goicoechea-Telleria, I.; Sanchez-Reillo, R.; Liu-Jimenez, J.; Blanco-Gonzalo, R. Attack Potential Evaluation in Desktop and Smartphone Fingerprint Sensors: Can They Be Attacked by Anyone? *Wireless Commun. Mobile Comput.* **2018**, *2018*, 1−16.
(31) Cao, K.; Jain, K. A. Hacking Mobile Phones Using 2D Printed Fingerprints. *MSU Technical Report*, 2016; MSU-CSE-16-2.
(32) Back, S.-W.; Lee, Y.-G.; Lee, S.-S.; Son, G.-S. Moisture-insensitive optical fingerprint scanner based on polarization resolved in-finger scattered light. *Opt. Express* **2016**, *24*, 19195−19202.
(33) Schultz, C. W.; Wong, J. X. H.; Yu, H. Z. Fabrication of 3D Fingerprint Phantoms via Unconventional Polycarbonate Molding. *Sci. Rep.* **2018**, *8*, 9613.
(34) Hong, S.; Hong, I.; Han, A.; Seo, J. Y.; Namgung, J. A new method of artificial latent fingerprint creation using artificial sweat and inkjet printer. *Forensic Sci. Int.* **2015**, *257*, 403−408.
(35) Dresselhaus, M. S.; Dresselhaus, G.; Saito, R.; Jorio, A. Raman spectroscopy of carbon nanotubes. *Phys. Rep.* **2005**, *409*, 47−99.
(36) Bandaru, P. Electrical Properties and Applications of Carbon Nanotube Structures. *J. Nanosci. Nanotechnol.* **2007**, *7*, 1239−1267.
(37) Gracia-Espino, E.; Sala, G.; Pino, F.; Halonen, N.; Luomahaara, J.; Mäklin, J.; Tóth, G.; Kordás, K.; Jantunen, H.; Terrones, M.; Helistö, P.; Seppä, H.; Ajayan, P. M.; Vajtai, R. Electrical transport and field-effect transistors using inkjet-printed SWCNT films having different functional side groups. *ACS Nano* **2010**, *4*, 3318−3324.
(38) Bruner, S.; Xu, D.; Phillips, C. Drop Landing Accuracy Improvements in Inkjet Printed OLED Displays. *SID Symp. Dig. Tech. Pap.* **2007**, *38*, 1611−1612.
(39) Soltman, D.; Smith, B.; Kang, H.; Morris, S. J. S.; Subramanian, V. Methodology for inkjet printing of partially wetting films. *Langmuir* **2010**, *26*, 15686−15693.
(40) Völkel, S.; Huang, K. Dynamics of wetting explored with inkjet printing. *EPJ Web Conf.* **2017**, *140*, 09035.
(41) Ashbaugh, D. R. *Quantitative−Qualitative Friction Ridge Analysis*, 1st ed.; CRC Press: New York, 1999; pp 61−74.
(42) Abdouni, A.; Djaghloul, M.; Thieulin, C.; Vargiolu, R.; Pailler-Mattei, C.; Zahouani, H. Biophysical properties of the human finger for touch comprehension: influences of ageing and gender. *R. Soc. Open Sci.* **2017**, *4*, 170321.
(43) Gusev, V. G.; Demin, A.; Galina, L. M.; Mikhal'chenko, E. S. Study of electrical properties of human skin. *Biomed. Eng.* **2009**, *43*, 124−127.
(44) Wolfe, S.; Pederson, W.; Kozin, H. S. *Green's Operative Hand Surgery*, 6th ed.; Elsevier, 2010.
(45) Galbally, J.; Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. A high performance fingerprint liveness detection method based on quality related features. *Future Gener. Comput. Syst.* **2012**, *28*, 311−321.
(46) Maltoni, D.; Maio, D.; Jain, K. A.; Prabhakar, S. *Handbook of Fingerprint Recognition*; Springer: New York, 2003; p 348.
(47) Liu, J.-C.; Hsiung, Y.-S.; Lu, M. S.-C. A CMOS Micromachined Capacitive Sensor Array for Fingerprint Detection. *IEEE Sens. J.* **2012**, *12*, 1004−1010.

DOI: 10.1021/acsomega.9b00936
ACS Omega 2019, 4, 8626−8631