Hybrid Camouflaged Anticounterfeiting Token in a Paper Substrate

Antonio Ferraro, Giuseppe Emanuele Lio,* Mauro Daniel Luigi Bruno, Sara Nocentini, Maria Penolepe De Santo, Diederik Sybolt Wiersma, Francesco Riboli, Roberto Caputo,* and Riccardo Cristoforo Barberi*

Anticounterfeiting of goods is an urgent need both for luxury and cheap everyday life products. Their identification is usually based on overt technologies as printed codes, easy to produce but to be cloned as well. In this work, a standard QR-code printed on office paper but hidden by a plasmonic multilayer system is exploited. The covert label is then protected by a peculiar reading mechanism, which is only possible in specific illumination conditions. The overall photonic structure consisting of the metal –insulator –metal –insulator, the printed random QR code and the paper substrate results in a strong physical unclonable function (PUF) that provides a multi-level identification and authentication of goods ensuring uniqueness of nominally quasi-identical tags and resistance to tampering/cloning attacks. The proposed paper-based camouflage physical unclonable function (PC-PUF) can be easily fabricated by low cost and large area techniques paving the way for an easy integration in an industrial supply-chain as tags devoted to protect consumer merchandises.

1. Introduction

The development of new approaches for securing goods or services is a ground-breaking technological sector. Counterfeiting is largely present in everyday life with significant economic damage in sectors including fashion, agri-food, jewellery, and electronics.[1] A large number of protocols are frequently used to validate the realized anticounterfeiting labels combining different approaches as microscopy, emissivity, colors, and phosphorescence[2–6] which require a quite complex experimental apparatus. In a more simple approach, the consumer checks the genuineness of a label by simply taking its picture with a smartphone and comparing it with the responses enrolled in the seller database.[7,8] In this scenario, materials science assumes a key-role by enabling the realization of so called physical unclonable functions (PUFs) that, characterized by intrinsic and unpredictable randomness, provide reliable identification or authentication.[9–14] Numerous examples of PUFs are found in literature employing different materials like plasmonic nanoparticles,[6,15,16] random silver nano-islands,[17] fluorescent materials,[18] and intrinsic material defects.[5] Countless chemical processes have been harnessed to generate tags of different nature—from complicated ink formulations used in banknotes to biodegradable and edible architectures that can be included in capsules for medical use.[2,19–22] In general, physical unclonable functions are defined as individual physical signatures whose intrinsic unpredictability produces a unique and "unclonable" response when interrogated by a specific challenge, following the so-called challenge-response pair (CRP) scheme.[23–26] Depending on the number of responses associated to a physical unclonable function, its strength can be classified as "weak" or "strong."[27]

A. Ferraro, M. D. L. Bruno, M. P. De Santo, R. Caputo, R. C. Barberi
Physics Department
University of Calabria
Arcavacata di Rende (CS), Rende 87036, Italy
E-mail: antonio.ferraro@cnr.it; roberto.caputo@unical.it

A. Ferraro, M. D. L. Bruno, M. P. De Santo, R. Caputo, R. C. Barberi
Consiglio Nazionale delle Ricerche - Istituto di Nanotecnologia CNR-Nanotec
(CS), Rende 87036, Italy

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/admt.202201010.

DOI: 10.1002/admt.202201010

G. E. Lio, F. Riboli
Consiglio Nazionale delle Ricerche - National Institute of Optics
CNR-INO, Sesto Fiorentino (FI), Florence 50019, Italy
E-mail: lio@lens.unifi.it

G. E. Lio, S. Nocentini, D. S. Wiersma, F. Riboli
European Laboratory for Non-Linear Spectroscopy (LENS)
University of Florence
Via Nello Carrara 1, Sesto Fiorentino, Florence 50019, Italy

G. E. Lio, D. S. Wiersma
Physics Department
University of Florence
Via Sansone, 1, Sesto Fiorentino, Florence 50019, Italy

S. Nocentini, D. S. Wiersma
Istituto Nazionale di Ricerca Metrologica (INRiM)
Strada delle Cacce 91, Turin 10135, Italy

R. Caputo
Institute of Fundamental and Frontier Sciences
University of Electronic Science and Technology of China
Chengdu 610054, China

Once interrogated, weak PUFs produce at least one response as in case of anti-counterfeiting tags.[5,6] Strong PUFs instead are more complex systems that under interrogation produce a large number of independent responses from the same device.[23,28] In both cases, it is essential to create a database where the challenge-response pairs are stored and available on demand for the end-user to grant or deny authentication. A particular class of advantageous and secure physical unclonable functions is constituted by optical ones.[29–32] They typically rely on scattering materials that, when illuminated by coherent light, due to the mutual interference of a set of coherent wavefronts, generate a complex speckle pattern in the far field.[7,33,34] Hence, their working principle finds its basis in the mesoscopic physics of complex photonic systems[35,36] which allows their fabrication with different optical features. In this manuscript, we demonstrate a multi level secret tag that realizes a secure authentication via a strong optical PUF. A multilayer plasmonic nano-cavity[37] enables the camouflage of a QR code printed on office paper. The resulting photonic metastructure behaves as both strong PUF and hidden identification tag. It is worth noting that paper is rarely used as a substrate for optical devices. The optical cavity is composed of thin silver (Ag) and zinc oxide (ZnO) layers. Moreover, the random morphology of paper enables the formation of unique speckle patterns when illuminated with coherent light such as lasers.[29,38] The proposed paper-based camouflage PUF, which is low-cost but extremely complex, can be easily applied to protect and guarantee the uniqueness of consumer goods such as food, liquor and wine, books, letters, and parcels. In particular this work focus on anticounterfeiting strong PUF for transparent packages such as beverage and liquor bottles, perfume bottles, Murano vases, clear plastic packaging and boxes. In case of opaque package, we envision to use the proposed label as an external one (as the one present in clothes, watches, jewellery to name a few) embedded in transparent stickers irreversibly damaged under fraudulent removal. Thanks to the involved forensics authentication, the PC-PUF enables a new category of device that perfectly mixes anticounterfeiting labels and strong PUFs to identify and authenticate merchandises that can be tampered or cloned. Moreover, the choice of using paper as substrate allows an easy integration in an industrial supply-chain with the benefit of fabricating sustainable and eco-friendly tags thus avoiding the use of electronics such as RFID and NFC devices. The possibility to print, for example, random QR codes previously enrolled in suitable validation databases is an added value to further increase the security level.

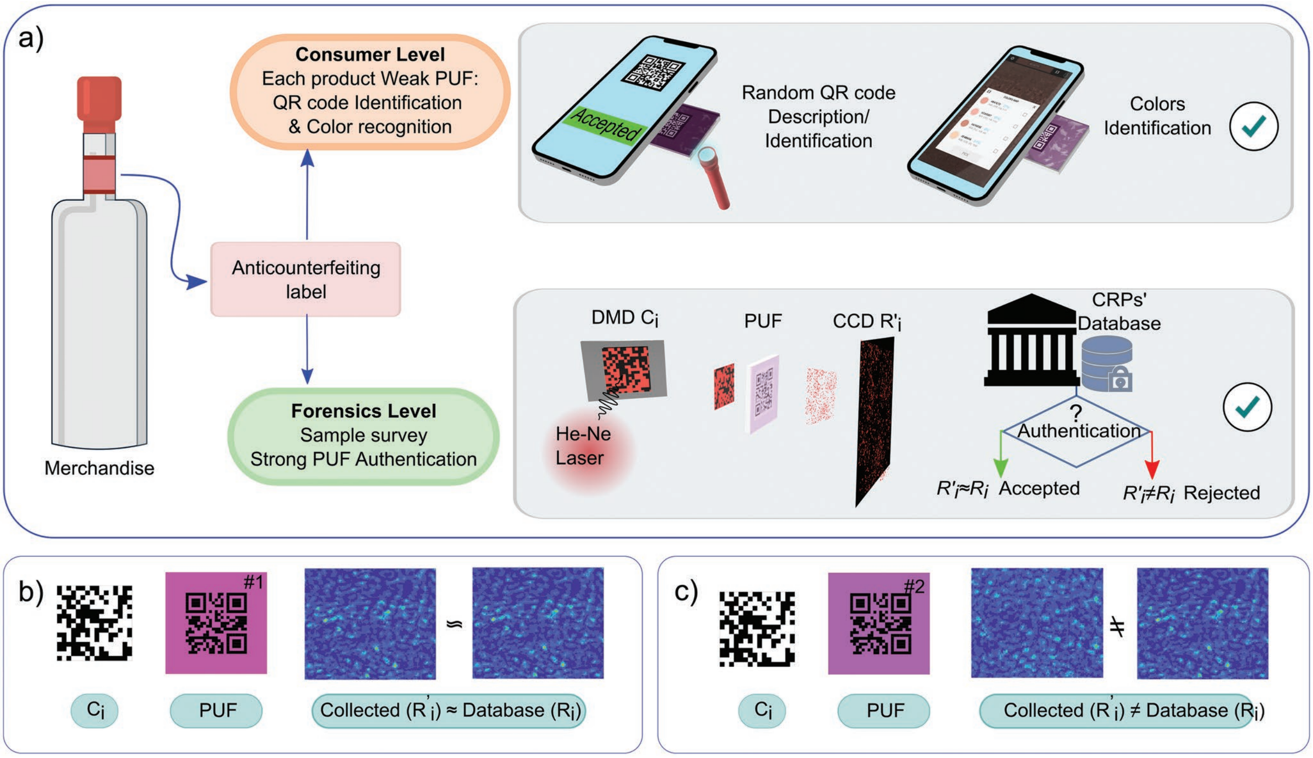


Figure 1. a) The sketch depicts the validation workflow of goods (merchandises) that are labeled with the proposed multi level paper-based camouflage PUFs (PC-PUFs). The consumer accesses to the first two identification levels by: i) using the QR-code readout system that is enabled illuminating the tag with light from the backside; or ii) using a suitable app to grab/capture the produced color hues when the tag is back-illuminated. Then, if the consumer and/or the sellers are still in doubt about the product validity, the third level can be considered. It consists in a forensic analysis made by a third party exploiting the challenge-response pairs scheme adapted to authenticate the genuineness of each label, or to check the validity in a sample survey of a batch of specific goods. PC-PUFs generate speckles that are compared to the one stored into the database allowing granting or denying depending on a preset threshold. In detail, the challenge-response pair procedure interrogates for example, PUF1 and PUF2 with the same challenge C_i, b) PUF1 that is the genuine produces a response ($R_i^{'}$) close to the stored one (R_i) and the good access is grant, c) PUF2 which looks similar to the previous one produces a speckle which is different from the stored one and the goods authentication is denied.

2. Multi Level Identification and Authentication Protocol

The proposed PC-PUFs exhibit different security levels: a twofold one represented by the generation of a random QR code and plasmonic structural colors ensuring the identification of the merchandise; and a third one consisting in the collection of the produced speckle patterns that guarantees a secure authentication based on strong PUFs. Furthermore, the QR code can be not only a descriptor including a "hyperlink" to the merchandise information but also the first identification level including an alphanumeric hashed code (SHA256). In addition, the encrypted hash allows the manufacturer including information about batch, production date and place, just to name a few, that make the QR code even more random in its generation.

Figure 1a illustrates the adopted identification workflow. The first step involves two factor identification and the readout approach consists in: i) using a smartphone and a light torch to illuminate the label from the backside and to read the information uploaded in the hidden QR code; ii) using a suitable smartphone application (open-source) to take a photo and grab the colors, generated by the plasmonic metamaterials, in the whole area. Then the obtained color map is compared with the one stored in the secure server. This step is easily accessible by the end user (consumer) by eventually using a messaging application to check the validity of the retrieved color identification.

The final step of the security workflow reaches a high level of product validation (indicates as "forensics" one) using the proposed camouflaged token as a strong physical unclonable function. In an eventual sample survey, a batch of identification tags are sent to a third party analysis laboratory that interrogates the labels following the challenge-response pair scheme and collects the authentication responses, that is, the speckle patterns. Then, the following step is to extract the binary keys $K_1 \dots K_i$ (related to the challenges $C_1 \dots C_i$ and responses $R_1 \dots R_i$) by adopting a Gabor hash filtering procedure which allows reshaping each collected speckle in a 1D binary array. The pairwise distance between each key $K_1 \dots K_i$ are then measured with the Hamming distance metric that is typically employed often used in bio-metrics and identification and authentication processes.[28] If keys are generated by different challenges probing a single PUF, the related fraction Hamming distances (FHD) statistical analysis creates "unlike" distribution whose properties gives information about the randomness of each key. Instead, the stability of the physical unclonable function can be estimated by probing the PUF by the same set of challenges and by measuring the FHD of the extracted keys, hence the "like" distribution can be reconstructed.[32,39,40] In this work, each physical unclonable function is probed by a finite set of challenges ($C_1 \dots C_i$) that are wavefronts modulated by employing a digital micro-mirror device (DMD), then light passes through them generating speckle patterns. More details are available in the Experimental Section. The challenge-response pairs stored in the database are used in real time to check the authenticity of the investigated label. Therefore, the access is granted only if the ware "fingerprint" is equal to the ones already stored, otherwise it is denied, see the sketch reported in Figure 1b. Indisputable is the case that someone can try to clone the QR code and the plasmonic cover layer. However, due to the fact that each paper substrate is different for each label, the cloned one produces different speckles and for example its response R_i' will be consequently different from the enrolled one R_i thus resulting in a denied access, see the depicted summary sketch in Figure 1c.

The presented tags can be considered as a new category of device that mixes weak and strong PUFs to identify and authenticate merchandises that can be tampered or cloned. Thanks to the paper substrate, they can be easily integrated with reduced cost into a supply chain with advantages respect to other electronic tags such as (RFID/NFC) because an electronic memory coupled to store the goods identity (ID) is not required, which means that it is not hackable with standard methods. Because the goods identity (ID) is inherently available on each tag, no enrollment phase is necessary to write it on the tag. On the other hand, only the manufacturers know the procedure to fabricate the paper-based camouflage PUFs (PC-PUFs) and it can be useful to avoid the well known night-shift issue. Moreover, in order to avoid any possibility for their tampering, the label can be placed on each good using an adhesive layer destructible upon removal from the substrate such as the PHED (peeled off layer by layer when removed), that possesses the feature that if peeled off layer by layer when removed avoiding the label transferring or using the breakable PVC / egg shell material that are non-transferable and they pulverize themselves when removed. Finally, the stability of the proposed paper-based camouflage PUF (PC-PUF) can be further improved by using wet-strength paper which is resistant to water and humidity.

3. Results

The secrecy layer has been engineered by a numerical investigation performed by using a transfer matrix method (TMM) script implemented in a commercial software *Matlab*. The considered multi-layer plasmonic nano-cavity is constituted by 40 nm of Ag, ZnO with variable thickness, 40 nm of Ag, and finally 40 nm of ZnO. The incident wave is set to be unpolarized in order to resemble a common illumination condition, that is, ambient light or smartphone LED. When illuminated, the paper substrate strongly diffuses the impinging light thus hindering the collection of reflectance and/or transmittance spectra. In other words, it is not possible to retrieve the multilayer refractive index by using ellipsometry.[41] To study the optical properties of the metal–insulator–metal–insulator, we first considered glass as a substrate. **Figure 2**a reports the reflectance and transmittance at normal incidence obtained for a ZnO cavity of 120 and 140 nm, where a red-shift of the reflecance dip is observed by increasing thickness. This turns out in different structural plasmonic colors observed by naked eye covering the chromaticity diagram from red to light blue, as reported in Figure 2b. This color sensitivity as a function of the considered cavity thickness arises from the formation of surface plasmon polaritons (SPPs) at the two metal surfaces and of gap surface plasmons (GSPs) in the ZnO layer.[37,42] The 120 nm thick cavity made of ZnO exhibits a transmission peak at $\lambda = 631$ nm, very close to the laser wavelength utilized for the CRP analysis. For the second ZnO cavity, 140 nm thick, the transmission peak is centered at $\lambda = 702$ nm. Even if the thickness difference is only 20 nm, the produced structural

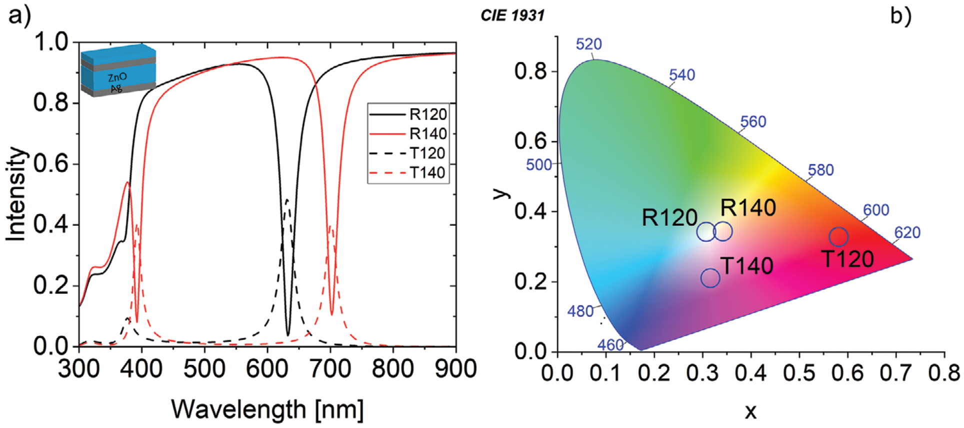


Figure 2. Numerical results for a multilayer nano-cavity composed by 40 nm thin silver (Ag) layer, 120 or 140 nm zinc oxide (ZnO) layer, 40 nm thin Ag layer, and 40 nm thin ZnO layer. a) Unpolarized reflection and transmission, b) related CIE chromaticity *xy*-coordinate plots with the corresponding points. In the inset a schematic view of the proposed multilayer.

plasmonic colors are completely different. From now on they are referred as PC-PUF-120 and PC-PUF-140. The same analysis has been performed by varying the thickness of the ZnO cavity in the range from 0 to 160 nm and the corresponding results are reported in Figure S1, Supporting Information.

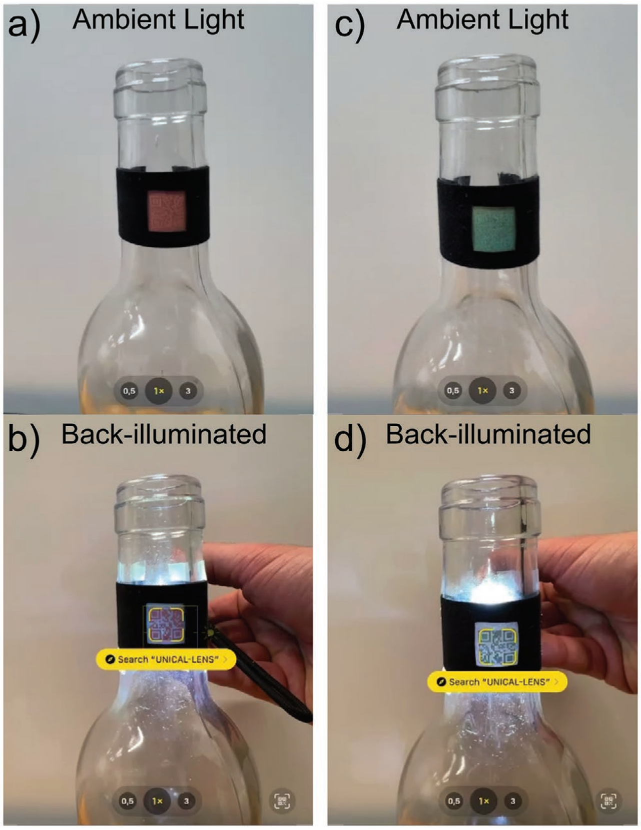


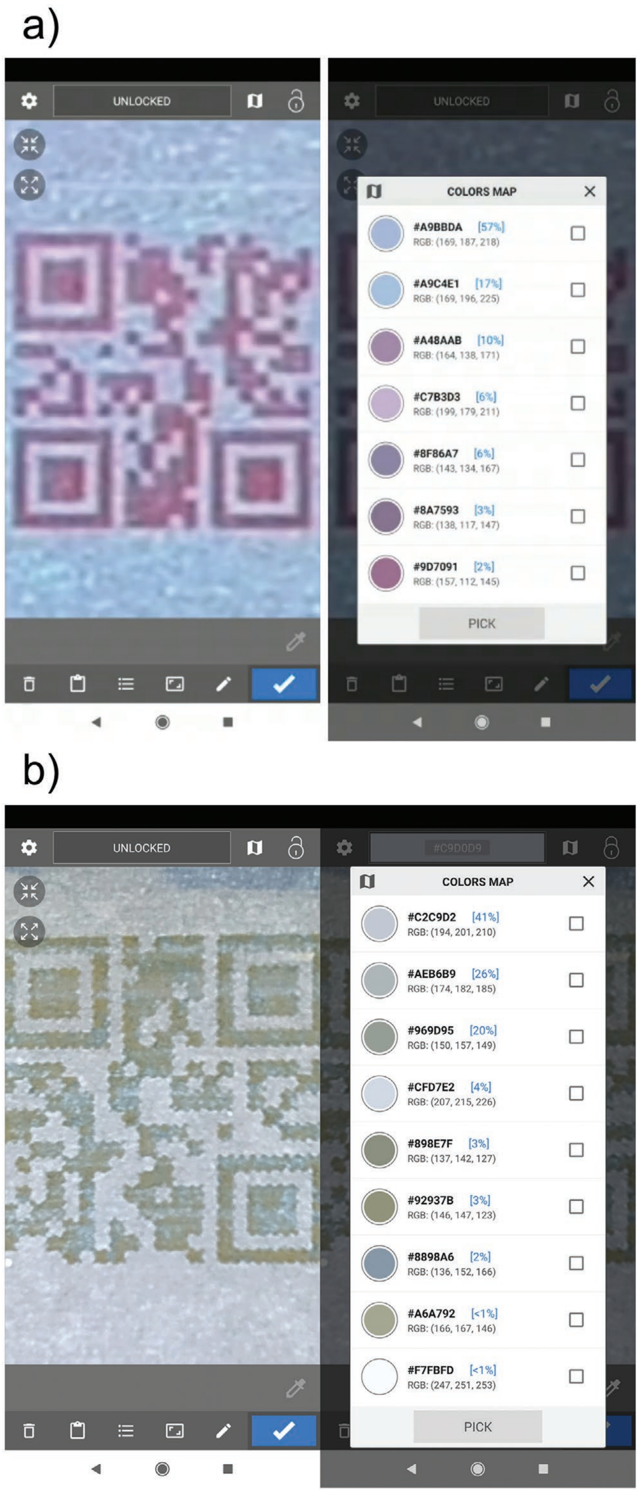
Figure 3. Snapshots of PUF having cavity thickness of 120 nm (PC-PUF-120) and 140 nm (PC-PUF-140), respectively, a,c) with ambient/reflection illumination where QR code cannot be resolved, b,d) with QR code reading using a white led torch behind PUFs.

Successively, the proposed paper-based camouflage PUFs (PC-PUFs) are realized on office paper using a commercial printer followed by sputtering deposition to allow very low cost and mass production. Additional details in Experimental Section. The fabricated anticounterfeiting tags are inserted into a label frame and then attached to the bottleneck of a liquor taking advantage of the flexibility and adaptability of the paper substrate required for many curved packaging. **Figure 3** reports frames of a smartphone screen during the QR code reading with a dedicated application. Due to the randomness and asperities of the paper substrate, the obtained structural colors are different with respect to the numerical ones. In fact, the PC-PUF-120 shows pinkish reflected colors while the PC-PUF-140 a gold one. Therefore, it is almost impossible also for the manufacturer to predict which will be the obtained colors. As expected, the multi-layer metamaterial camouflages the printed QR code which is slightly visible and cannot be resolved in presence of ambient illumination, see Figure 3a,c. By a retro-illumination of the PC-PUFs with a low cost white led torch, the QR code is easily resolved and correctly read by a smartphone application, showing in this case the encoded phrase “UNICAL-LENS”. This QR code, that is intentionally not random, has been chosen to demonstrate the operation of the proposed tag under different conditions.

The acquired videos, Movies S1 and S2, Supporting Information, are available in Supporting Information materials. This operation represents the first level of authenticity that is easily accessible by the end-user. It is worth noting that this level combines the versatility of printing random QR codes with the peculiar characteristics of plasmonic structural colors.

In a more general view of easy but robust operation, the other security level is guaranteed by the evaluation of color hues/shadows as reported in **Figure 4**. Indeed, when operated by the led torch, they show colors. This analysis is easily performed by using a smartphone equipped with a specific freeware application. Starting from photographs of the proposed tag, the app retrieves the colors of the whole area returning their hexadecimal code and percentage.

When illuminated with a white torch behind it, for the PC-PUF-120 it is obtained 57% for color #A9BBDA and 17%



a)

#A9BBDA [57%] RGB: (169, 187, 218) □
#A9C4E1 [17%] RGB: (169, 196, 225) □
#A48AAB [10%] RGB: (164, 138, 171) □
#C7B3D3 [6%] RGB: (199, 179, 211) □
#8F86A7 [6%] RGB: (143, 134, 167) □
#8A7593 [3%] RGB: (138, 117, 147) □
#9D7091 [2%] RGB: (157, 112, 145) □

b)

#C2C9D2 [41%] RGB: (194, 201, 210) □
#AEB6B9 [26%] RGB: (174, 182, 185) □
#969D95 [20%] RGB: (150, 157, 149) □
#CFD7E2 [4%] RGB: (207, 215, 226) □
#898E7F [3%] RGB: (137, 142, 127) □
#92937B [3%] RGB: (146, 147, 123) □
#8898A6 [2%] RGB: (136, 152, 166) □
#A6A792 [<1%] RGB: (166, 167, 146) □
#F7FBFD [<1%] RGB: (247, 251, 253) □

Figure 4. Color map recognition when retro-illuminated with a white LED torch: a) for PC-PUF-120 and b) PC-PUF-140.

for #A9C4E1, see Figure 4a. In case of the PC-PUF-140, despite a small difference of 20 nm of the ZnO layer, the colors are completely different resulting 41% for #C2C9D2 and 26% for #AEB6B9, as reported in Figure 4b. A tolerance in the "HEX" code number (color hues) and percentage could be applied in order to avoid discrepancy between different smartphones. Moreover, it is not appropriate to take in consideration colors with percentages below 15%. In case of operations into laboratory or supply chain, colorimeters can be easily utilized, as already performed in industry, ensuring consistency and reproducibility.

Next, a forensic characterization according to the challenge-response pairs (CRPs) scheme was performed on the proposed paper-based camouflage PUFs by using 2000 challenges. The corresponding 2000 responses were collected, post-processed and finally the extracted binary keys were analyzed using the Hamming distance metric. The entire process returns as an output the fractional Hamming distances (FHD) distributions shown in **Figure 5**. Herein, we consider only PC-PUF-120, namely the label with the printed QR-code covered by a ZnO cavity 120 nm thick. For this analysis, the sample is indicated as PUF1. When illuminated with the set challenges, produces "unlike" responses close to a FHD mean value of 0.5 meaning that the entire set of $R_1 \ldots R_i$ is unique. By repeating this procedure the "like" responses are centered at 0.135, meaning that each response is similar to the enrolled one and stable in

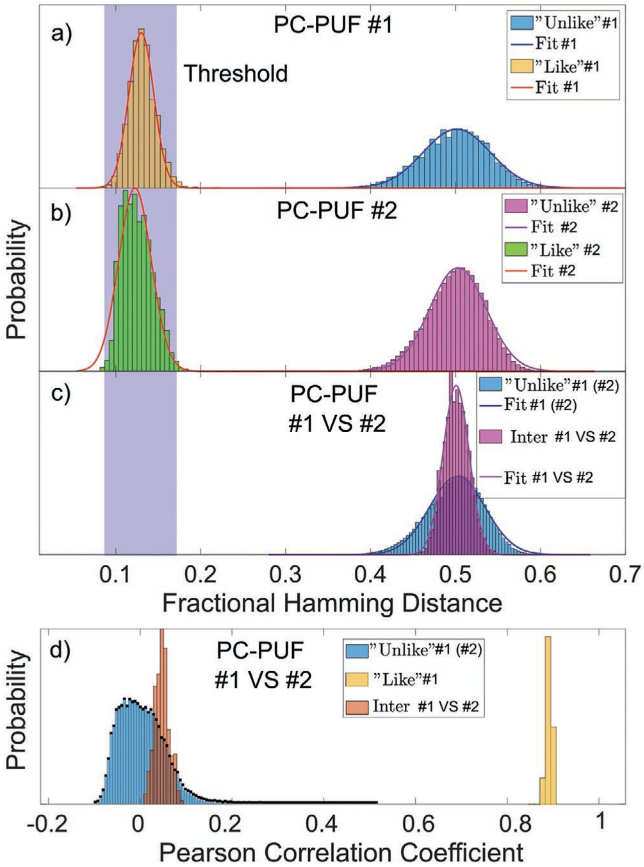


Figure 5. The distributions for two PC-PUF-120 made on different pieces of paper show: a) PUF #1 unlike FHD distribution centered at 0.5 and the like one at 0.135, blue and yellow histograms respectively. b) Unlike (magenta) and like (green) FHD distributions for PUF #2 centered at 0.5 and 0.127. c) Comparison of #1 and #2 shows both unlike and like FHD distributions centered at 0.5. d) The Pearson correlation coefficient distribution evaluated on the CRPs collected by PUF #1 and PUF #2 shows mean values close to zero highlighting the differences between the two labels.

time. As mentioned above, this mean value fixes the threshold for the label validation, see the blue and yellow histograms in Figure 5a, respectively. The mean values are retrieved by fitting the histograms with a Gaussian distribution reported as blue and red solid lines in the plot.

The same test has been repeated on another label realized as the first one (PUF1), hence with the same multilayer structure, but on a different piece of paper which is now indicated as PUF2. As in the previous case, the latter presents an unlike FHD distribution close to 0.5 and a like one centered at 0.127—see the magenta and green histograms—and related fits (purple and red solid lines) in Figure 5b, respectively. By comparing the obtained responses of the two PC-PUF-120 interrogated with the same set of challenges, the forensics analysis reveals the large difference between such responses and the related inter distribution is centered at 0.5, see Figure 5c. Therefore, the analysis highlights as two labels that look identical to the naked eye provide completely different responses if interrogated with coherent light. This result thwarts any cloning attempt. Another possible approach to evaluate the likeness/unlikeness of the two analyzed PC-PUFs is the Pearson correlation coefficient (Figure 5d). It directly compares the raw images without any post-processing, hence no other correlations or randomness are introduced. Such further evaluation reflects the results shown previously thus confirming the differences between the two labels.

4. Conclusions

The proposed PC-PUFs exhibits multi security identification and authentication levels based on QR code, color readout, and speckle analysis. These are intended to different possible users: the first and second one are accessible to end-users and not specialized persons with a double check on the label genuineness by interrogating a specific repository where all the information, for example, QR code and color association, are stored. The third one is a forensic level validation because it requires a sophisticated apparatus and experts in the field and can be adopted for legal actions or in a even more common use for a sample survey. The proposed physical unclonable functions represent an ideal candidate for the protection of merchandise, with transparent or opaque packages, thanks to their low cost, lower than 1$, and large scale production possibilities. As a perspective, by suitable multilayer structure engineering, the proposed technology can operate in front-illumination condition offering countless applications.

5. Experimental Section

Samples Fabrication: Fabrication began by printing a QR code on office paper by using commercial office laser printing. On top of the printed paper a multi layer nano-cavity had been deposited using sputtering technique (model Kenosistec KC300C). At first a silver (Ag) layer of 40 nm was deposited with the following parameters: vacuum 7×10^{-6}, DC power 100 W for 82 s. Successively 120 and 140 nm of ZnO were deposited using the RF cathode at a power of 80 W and time of 37 min 37 s and 43 min 53 s, respectively. Then 40 nm of Ag followed by 40 nm of ZnO.

CRP Characterization: Experimental Setup: A red laser beam with wavelength $\lambda = 633$ nm (power 5 mW) propagated through a series of lenses, polarizers, and irises. The beam, after beam spot magnification by a beam-expander, impinged on a DMD used for the challenge (C_i) generation by means of an intensity modulation. The beam wave acquired individual spatial features for each individual C_i, that directly interrogated the scattering PC-PUF sample illuminating an area with the same size of the printed QR-code. The light propagation interference produced a transmission optical pattern in the far field named speckle pattern. This constituted the PUF response R_i, that is collected in cross polarized configuration in order to remove any non-scattered light. This pattern was collected by a CCD camera. Here, a 270 × 360 px camera with 40 FPS for this task was used (see Figure S2, Supporting information).

Supporting Information

Supporting Information is available from the Wiley Online Library or from the author.

Acknowledgements

A.F., M.D.L.B., M.P.D.S., R.C., and R.C.B. thank project : "DEMETRA – Sviluppo di tecnologie di materiali e di tracciabilitá per la sicurezza e la qualitá dei cibi" PON ARS01 00401. The LENS research group thanks the FASPEC (Fiber-Based Planar Antennas for Biosensing and Diagnostics), the project "Complex Photonic Systems" (DFM.AD005.317), and the project "Highly Secure Nonlinear Optical PUFs" supported by the US Air Force Office of Scientific Research (AFOSR) under Grant No. FA9550-21-1-0039. G.E.L. also thanks the research project "FSE-REACT EU" financed by National Social Fund–National Operative Research Program and Innovation 2014-2020 (D.M. 1062/2021), personal Grant number 10-G-15049-2.

Open access funding provided by Universita della Calabria within the CRUI-CARE Agreement.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

A.F. conceived the idea and coordinated the overall research effort. A.F., G.E.L, and M.D.L.B carried out the experiments. G.E.L, S.N., and F.R. designed and implemented the experimental setup for the challenge response pairs scheme, and they collected, studied and analyzed the speckle data. M.P.D.S., D.S.W., R.C., and R.C.B. discussed the results. The manuscript was written by A.F. and G.E.L. with the input from all authors. The project was supervised by R.C.B.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Keywords

anticounterfeiting tags, paper substrate, physical unclonable function, plasmonic metamaterials, QR code, speckle

Received: June 22, 2022
Revised: September 6, 2022
Published online:

[1] D. Grajales Pérez-y-Soto, Counterfeiting and piracy in 2021—the global impact, World Trademark Review, **2021**.
[2] J. W. Leem, M. S. Kim, S. H. Choi, S.-R. Kim, S.-W. Kim, Y. M. Song, R. J. Young, Y. L. Kim, *Nat. Commun.* **2020**, *11*, 328.
[3] Y. Lin, H. Zhang, J. Feng, B. Shi, M. Zhang, Y. Han, W. Wen, T. Zhang, Y. Qi, J. Wu, *Small* **2021**, *17*, 2100244.
[4] H. Im, J. Yoon, J. Choi, J. Kim, S. Baek, D. H. Park, W. Park, S. Kim, *Adv. Mater.* **2021**, *33*, 2102542.
[5] Q. Li, F. Chen, J. Kang, P. Wang, J. Su, F. Huang, M. Li, J. Zhang, *Adv. Photonics Res.* **2021**, *3*, 2100207.
[6] Q. Li, F. Chen, J. Kang, J. Su, F. Huang, P. Wang, X. Yang, Y. Hou, *Adv. Funct. Mater.* **2021**, *31*, 2010537.
[7] R. Arppe, T. J. Sørensen, *Nat. Rev. Chem.* **2017**, *1*, 0031.
[8] A. Ferraro, M. D. L. Bruno, G. Papuzzo, R. Varchera, A. Forestiero, M. P. De Santo, R. Caputo, R. C. Barberi, *Nanomaterials* **2022**, *12*, 1279.
[9] R. Maes, I. Verbauwhede, in *Towards Hardware-Intrinsic Security*, Springer, Berlin **2010**, pp. 33–37.
[10] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, *Proc. IEEE* **2014**, *102*, 1126.
[11] H. J. Bae, S. Bae, C. Park, S. Han, J. Kim, L. N. Kim, K. Kim, S.-H. Song, W. Park, S. Kwon, *Adv. Mater.* **2015**, *27*, 2083.
[12] G. Petriashvili, M. P. De Santo, L. Devadze, T. Zurabishvili, N. Sepashvili, R. Gary, R. Barberi, *Macromol. Rapid Commun.* **2016**, *37*, 500.
[13] G. Petriashvili, M. P. De Santo, R. J. Hernandez, R. Barberi, G. Cipparrone, *Soft Matter* **2017**, *13*, 6227.
[14] Y. Gao, S. F. Al-Sarawi, D. Abbott, *Nat. Electron.* **2020**, *3*, 81.
[15] J. Kim, J. M. Yun, J. Jung, H. Song, J.-B. Kim, H. Ihee, *Nanotechnology* **2014**, *25*, 155303.
[16] G. Emanuele Lio, A. De Luca, C. P. Umeton, R. Caputo, *J. Appl. Phys.* **2020**, *128*, 093107.
[17] V. Caligiuri, A. Patra, M. P. De Santo, A. Forestiero, G. Papuzzo, D. M. Aceti, G. E. Lio, R. Barberi, A. De Luca, *ACS Appl. Mater. Interfaces* **2021**, *13*, 49172.
[18] Y. Liu, Y. Zheng, Y. Zhu, F. Ma, X. Zheng, K. Yang, X. Zheng, Z. Xu, S. Ju, Y. Zheng, T. Guo, L. Qian, F. Li, *ACS Appl. Mater. Interfaces* **2020**, *12*, 39649.
[19] B. Yoon, D.-Y. Ham, O. Yarimaga, H. An, C. W. Lee, J.-M. Kim, *Adv. Mater.* **2011**, *23*, 5492.
[20] K. Nakayama, J. Ohtsubo, *Opt. Eng.* **2012**, *51*, 040506.
[21] L. Romano, A. Portone, M.-B. Coltelli, F. Patti, R. Saija, M. A. Iatí, G. Gallone, A. Lazzeri, S. Danti, O. M. Maragó, A. Camposeo, D. Pisignano, L. Persano, *Nat. Commun.* **2020**, *11*, 5991.
[22] J. Fei, R. Liu, *Mater. Sci. Eng., C* **2016**, *63*, 657.
[23] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Science* **2002**, *297*, 2026.
[24] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, C. Yang, *Sci. Rep.* **2013**, *3*, 3543.
[25] R. Arppe-Tabbara, M. Tabbara, T. J. Sørensen, *ACS Appl. Mater. Interfaces* **2019**, *11*, 6475.
[26] G. E. Lio, S. Nocentini, L. Pattelli, E. Cara, D. Sybolt Wiersma, U. Rührmair, F. Riboli, arXiv:2208.02906, **2022**.
[27] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, R. J. Young, *Appl. Phys. Rev.* **2019**, *6*, 011303.
[28] J. Daugman, *Pattern Recognit.* **2003**, *36*, 279.
[29] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, *Science* **2002**, *297*, 2026.
[30] B. Škorić, P. Tuyls, W. Ophey, in *International Conf. on Applied Cryptography and Network Security*, Springer, Berlin **2005**, pp. 407–422.
[31] P. Tuyls, B. Škoric, T. Kevenaar, *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, Springer Science & Business Media, Berlin **2007**.
[32] R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assawaworrarit, C. Yang, *Sci. Rep.* **2013**, *3*, 1.
[33] J. W. Goodman, *JOSA* **1976**, *66*, 1145.
[34] H. Cao, Y. Eliezer, *Appl. Phys. Rev.* **2022**, *9*, 011309.
[35] F. Riboli, N. Caselli, S. Vignolini, F. Intonti, K. Vynck, P. Barthelemy, A. Gerardino, L. Balet, L. H. Li, A. Fiore, M. Gurioli, D. S. Wiersma, *Nat. Mater.* **2014**, *13*, 720.
[36] F. Riboli, F. Uccheddu, G. Monaco, N. Caselli, F. Intonti, M. Gurioli, S. Skipetrov, *Phys. Rev. Lett.* **2017**, *119*, 043902.
[37] G. E. Lio, A. Ferraro, M. Giocondo, R. Caputo, A. De Luca, *Adv. Opt. Mater.* **2020**, *8*, 2000487.
[38] A. O. Pino, J. Pladellorens, J. F. Colom, *Proc. SPIE* **2010**, *7387*, 73871W.
[39] T. M. Cover, *Elements of Information Theory*, John Wiley & Sons, Hoboken, NJ **1999**.
[40] C. Böhm, M. Hofer, *Physical Unclonable Functions in Theory and Practice*, Springer Science and Business Media, Berlin **2012**.
[41] G. E. Lio, G. Palermo, R. Caputo, A. De Luca, *RSC Adv.* **2019**, *9*, 21429.
[42] G. E. Lio, A. Ferraro, T. Ritacco, D. M. Aceti, A. De Luca, M. Giocondo, R. Caputo, *Adv. Mater.* **2021**, *33*, 2008644.