IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 31, 2022, accepted February 14, 2022, date of publication February 21, 2022, date of current version March 9, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3153051

Smart Optical Sensors for Internet of Things: Integration of Temperature Monitoring and Customized Security Physical Unclonable Functions

LÍLIA M. S. DIAS[1], JOÃO F. C. B. RAMALHO[1], TIAGO SILVÉRIO[1,2], LIANSHE FU[1,3], RUTE A. S. FERREIRA[1], AND PAULO S. ANDRÉ[4], (Senior Member, IEEE)

[1]Department of Physics and CICECO - Aveiro Institute of Materials, University of Aveiro, 3810-193 Aveiro, Portugal
[2]Instituto de Telecomunicações, University of Aveiro, 3810-193 Aveiro, Portugal
[3]Department of Chemistry, University of Aveiro, 3810-193 Aveiro, Portugal
[4]Department of Electrical and Computer Engineering and Instituto de Telecomunicações, Instituto Superior Técnico, University of Lisbon, 1049-001 Lisbon, Portugal

Corresponding authors: Rute A. S. Ferreira (rferreira@ua.pt) and Paulo S. André (paulo.andre@lx.it.pt)

This work was supported in part by the CICECO—Aveiro Institute of Materials under Project UIDB/50011/2020, Project UIDP/50011/2020, and Project LA/P/0006/2020; in part by the Instituto de Telecomunicações under Grant UIDB/50008/2020 and Grant UIDP/50008/2020; and in part by the Graphsense funded by National Funds through the FCT/MEC (PIDDAC) when appropriate Co-Financed by FEDER under the PT2020 Partnership through European Regional Development Fund (ERDF) in the Frame of Operational Competitiveness and Internationalization Program (POCI) under Grant POCI-01-0145-FEDER-032072. The work of Lília M. S. Dias was supported by the SOLPOWINS under Grant PTDC/CTM-REF/4304/2020.

ABSTRACT Nowadays, the Internet of Things (IoT) has an astonishingly societal impact in which healthcare services stand out. Amplified by the COVID-19 pandemic scenario, challenges include the development of authenticatable smart IoT devices with the ability to simultaneously track people and sense in real-time human body temperature aiming to infer a health condition in a contactless and remote way through user-friendly equipment such as a smartphone. Univocal smart labels based on quick response (QR) codes were designed and printed on medical substrates (protective masks and adhesive) using flexible organic-inorganic luminescent inks. Luminescence thermometry and physical unclonable functions (PUFs) are simultaneously combined allowing non-contact temperature detection, identification, and connection with the IoT environment through a smartphone. This is an intriguing example where luminescent inks based on organic-inorganic hybrids modified by lanthanide ions are used to fabricate a smart label that can sense temperature with remarkable figures of merit, including maximum thermal sensitivity of $S_r = 1.46\ \%K^{-1}$ and temperature uncertainty of $\delta T = 0.2$ K, and an authentication methodology accuracy, precision, and recall of 96.2%, 98.9%, and 85.7%, respectively. The methodology proposed is feasibly applied for the univocal identification and mobile optical temperature monitoring of individuals, allowing the control of the access to restricted areas and the information transfer to medical entities for post medical evaluation towards a new generation of mobile-assisted *eHealth* (*mHealth*).

INDEX TERMS eHealth, IoT, luminescence, mHealth, physical unclonable functions, QR codes, smart labels, sensors, thermometry, authentication.

I. INTRODUCTION

The information and communication technologies, and in particular, the Internet of Things (IoT), are progressively being included in nowadays society along with mobile systems, impacting our daily life in distinct fields such as industry, education, transportation, and healthcare [1], [2]. In 2011, 50 billion IoT devices were predicted to be connected by 2020, with the actual number being slightly higher than 12 billion [3]. The main barriers to entry for the technology that account for this deviation in the forecast are related to security and communications aspects.

The associate editor coordinating the review of this manuscript and approving it for publication was Chao Zuo.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

Incorporating IoT functionalities (temperature sensors and ID tags) with mobile devices can be a window of opportunity to tackle the security and communication aspects, helping to remove the barriers to the dissemination of the IoT devices [3]. Enlarged by the COVID-19 pandemic scenario, healthcare services standout and the concepts of *eHealth* and *mHealth* (mobile-assisted *eHealth*) arose [4], [5], being more and more explored towards the development of effective low-cost and sustainable systems that promote healthcare provision [6].

New technologies that rely on the identification of individuals based on personal information must address safety measures, and this is particularly important in *eHealth* systems, that besides using personal information, also generate new data (healthcare-related) that must be kept private and safe [7], [8]. Therefore, the security of the information storage and the authentication of the systems is required. The onset of the COVID-19 pandemic brought additional challenges associated with personal identification for access to restricted areas, due to the wearing of face-covering artifacts such as protection masks [9]. Face covering introduced difficulties in the identification and tracking of people by the face recognition algorithms. The National Institute of Standards and Technology evaluates the performance of these algorithms on the identification of people wearing masks, resulting in error rates between 5% and 50% when matching photos of the same person with and without a digitally applied mask [9].

Conventional authentication approaches include the use of non-volatile or battery-backed memory to store information that can be authenticated using hardware cryptographic operations. These approaches are power expensive and less suited for real-time applications with limited resources [10]. Physical unclonable functions (PUFs) appear as a solution to mitigate the disadvantages of such conventional approaches [9]. This concept arises as a new type of cryptographic approach, making use of the unique physical disorders that are introduced on the manufacturing of a device, generating, through them, a ''fingerprint'' of the device that can be subject to authentication processes ([9] and references therein). This approach is based on a black-box *challenge-response* system, where an external stimulus is applied to the device. The *challenge* is applied, and specific parameters measured, constituting an unpredictable and unique *responses* of the device to the *challenge*. It is considered a black-box description since the factors that are involved in the generation of the *response* are unidentified but result from the internal manufacturing variability of the device itself. This underlies the safety of PUFs, as these internal factors, in addition to being unknown, are difficult to estimate and therefore to replicate [8]. The PUFs are easier to fabricate, require less power consumption, and do not require expensive hardware [8], [10], [11]. Security aspects related to PUF-based labels have been addressed in the literature [12], [13] together with their use in authentication protocols [11], [14], [15]. Additionally, a PUF can still work in combination with the recognition of biometric parameters to further enhance security and avoid unwanted usage from non-authorized personnel. The use of these in authentication applications requires a so-called strong PUF with many *challenge-response* pairs [16].

Distinct PUFs can be produced by changing the initial conditions, that encompass the materials, the components of the system, the measured physical parameters, the origin of the variability, among others. So far, the electronic domain has been leading the development of PUFs [17]. Optical PUFs arose as a viable alternative, providing a stronger unclonability as they generate more complex responses, which further enhances the security of the system. The main challenge for optical PUFs is still to create authentication methodologies capable of transforming the optical *response* into a random digital key that is uncorrelated with the *responses* from different PUFs, as this is the basic principle of unclonability [17], [18]. So far, few reports have already managed a complete verification with certified standards of both unpredictability and uncorrelation of the generated keys from optical PUFs [15], [18]. Another limitation of PUFs is the need for hardware capable of measuring its *response*, which in this case is an optical signal. The possibility of using mobile phones is an opportunity to bridge the gap between PUF and the IoT environment. This is possible due to the mobile phones high-resolution camera (charge-coupled device, CCD) capable of reading the optical response, the enormous computing power capable of processing it, and the available communication interface that allows to connect everything to external networks.

Besides the challenges associated with personal identification, the current pandemic scenario also imposed restrictions on the maximum corporal temperature of individuals to access several areas or events, requiring certification that this value is under a defined threshold that indicates the absence of fever. Among the distinct sensing technologies, optical sensors appear as alternatives to electronic ones in distinct scenarios (including COVID-19 triages) because they are contactless allowing that the same thermometer can be used for several individuals without sanitary concerns, and provide faster response time, and larger-scale measurements [19], [20]. Thus, more than one person can be monitored in a short time. The NIR thermal cameras are one of the main devices used due to the fast response times and non-interference to electromagnetic fields in the working environment. Nonetheless, the thermal cameras are sensitive to surrounding ambient conditions such as stray light, reflected radiation, flame, or gas steam that can generate temperature uncertainties up to 1-8% [21]. The recent evolution of luminescence thermometry characterized by high spatial resolution ($<10\ \mu$m), short acquisition time (<1 ms), and high relative thermal sensitivity ($>\ 1\,\% \cdot \mathrm{K}^{-1}$) towards mobile-optical (mOptical) sensing mediated by smartphones appear as an intriguing strategy to enable large-scale sensing and tracking mediated by the user [20], [22].

In the scenario where concurrent authentication and thermal sensing are required, challenges for *eHealth* and *mHealth* encompass the development of authenticatable smart labels that can sense physical parameters (e.g., body temperature) to infer a health condition in a remote way and through user-friendly equipment such as a smartphone. Among labels, luminescent quick response (QR) codes appear as the ideal interface between the user and the IoT as the reading is available through a smartphone [23]–[26]. As an added benefit, the judicious choice of the luminescent inks offers the possibility to print the QR codes on virtually any substrate and the temperature sensing [16] with maximum thermal sensitivity values among the best values in the literature for luminescence-based thermometers [20], [23], [26]. Moreover, the production of luminescent QR codes has several freedom levels (*e.g.,* luminescent material, deposition method, size, and shape) which contribute to the differences in their luminescence-based *responses*, placing them as interesting candidates to optical PUFs. Regarding authentication, few reports refer to the combination of PUFs and luminescent QR codes. Tags of microscopic luminescent particles (Eu^{3+} and Tb^{3+} based phosphors) were produced using different methods and materials to generate unpredictable PUF *responses* [12]. Also, randomly distributed nanoparticles were used as pinning points to attach semiconductor quantum dots with RGB emission (CdSe/CdS/CdZnS, ZnCdSe/CdZnS, ZnCdS/CdZnS), generating random patterns [13]. Although luminescent QR codes were already explored as luminescent temperature sensing labels or as univocal labels, the exploitation of unclonability and authentication of luminescent QR codes using the same sensing layer is a novelty.

In this work, we report the first example in which the same QR code is an unclonable label able to sense temperature and suitable for an authentication application using a photo taken with a smartphone with remarkable figures of merit, combining the concepts of PUFs with mOptical luminescence thermometry. The selected luminescent materials are based on organic-inorganic hybrid (di-ureasils) inks prepared at room temperature with tunable optical and structural properties [24]. Regarding biocompatibility, di-ureasils have been addressed as biocompatible materials in recent literature [27]. The possibility of incorporating lanthanide (*e.g.,* $Ln^{3+} = Eu^{3+}$) complexes comprising suitable ligands provides pure color emission (full-width-at-half-maximum, fwhm<4 nm) in the visible spectral regions. Moreover, the radiation harvesting, and the large Stokes shift provided by the ligands ensure efficient Ln^{3+} emission under the lower-excitation powers typical of commercial light-emitting diodes (LEDs). The combined use of smartphones and LEDs is a sustainable approach to the industry, societal acceptance, and widespread use, providing a unique opportunity to develop effective low-cost, and sustainable systems for *mHealth* and *eHealth*. In addition, this work provides evidence of the use of luminescent PUFs for enhanced security and simultaneous mOptical temperature sensing.

II. TEMPERATURE OPTICAL SENSOR WITH CUSTOMIZED PUF FOR IoT

A. CONCEPT AND DESIGN

The design of the univocal smart labels started with the creation of a regular QR code and its customization to be processed with selected aqueous-based inks (Fig. 1). Conjugating the two functionalities of identification and contactless temperature monitoring for access control, a regular non-luminescent black/white QR code was transformed with the inclusion of a smart finder pattern processed using a monochromatic luminescent ink based on organic-inorganic hybrid (termed as di-ureasil) [28], [29] doped with a well-characterized Eu^{3+}-based beta-diketonate complex [30], [31] and Tb^{3+}- salicylic acid complex [24], [32] (Supplemental Material, Fig. S1). The rationale for the selection of these inks (hereafter termed as dU6Eu and dU6Tb, respectively) lies in their remarkable properties from the mechanical and thermal stabilities [24], [32], [33] to the high emission quantum yield (up to 89% [33]), depending on the processing methods. The selected inks are photo- and chemical-stable even upon accelerated aging tests performed under controlled relative humidity and temperature and prolonged continuous solar irradiation (AM1.5G, 1000 Wm^{-2}) [24]. The inks are also resilient to conventional sanitized processes involving exposure to UV radiation or the use of alcohol-based solutions. The di-ureasils are known to prevent photodegradation upon UV exposure [34]–[36]. In the case of alcoholic-based solutions, we note that only the precursors are soluble. After gelification, the hybrid matrix (di-ureasil) cannot be easily dissolved in ethanol, due to its polymeric nature. Moreover, the case study is based on a disposable mask, so the use of several sanitized processes is in principle excluded.

The strategy to combine the need for two luminescent inks is to provide a more complex *challenge-response* behavior from the physical disorder present in the PUF. The emission patterns arising from the red and green inks are distinct and depend on the excitation wavelength. Therefore, the generated patterns change according to the excitation wavelength, creating a strong PUF, as detailed next. From the optical point of view, the dU6Eu (and dU6Tb) is transparent under daylight and reveals a bright red (green) color visible to the naked eyes under UV illumination (Fig. 1). The unclonability and authentication will be explored using a smartphone and a strong PUF suitable for authentication. The *challenges* lie on excitation wavelength in the UV/blue spectral range (250-420 nm and 465 nm) and the *responses* are the activated random emission shape of the location pattern accessible under UV/blue LEDs illumination. Under daylight the inks are transparent, and the smart location patterns are hidden. Moreover, the dependence of the emission color [26] of the smart location pattern will be explored to design a luminescent ratiometric thermometer. The dU6Eu luminescent material exhibits color coordinates that depend on the temperature, changing its intensity as the temperature varies. The correlation between the temperature of the exhaled air

during breathing measured at the mask where the label is placed permits to infer corporal temperature [37] using commercial CCD cameras, such as from a smartphone or closed-circuit television (CCTV), Fig. 1.

The concept here proposed can be applied also to substrates such as medical adhesives for *eHealth/mHealth* [26]. Remote medical care through temperature monitoring in scenarios such as post-diagnosis or post-surgery, where direct and authenticated contact with the medical entity is essential can be assured. In the case of the COVID-19 pandemic scenario, the individual protection masks will enable tracking and temperature sensing of employees of a company, to enable/restrict access to controlled areas or events based on the identification and body temperature (Fig. 1.d).

B. MATERIALS AND PROCESSING

The materials used were α, ω-Diaminepoly (oxyethylene-co-oxypropylene) (ED-600, Huntsman), 3-isocyanatepropyltriethoxysilane (ICPTES, 95%, Aldrich), and $EuCl_3 \cdot 6H_2O$ (Aldrich) that are commercially available. Tetrahydrofuran (THF) and absolute ethanol (EtOH) were used as solvents. All chemicals were used as received without purifications and distilled water was used throughout the experiments. The organic-inorganic hybrid non-hydrolyzed precursor, d-UPTES(600) [28], and the Eu^{3+} and Tb^{3+} complexes were synthesized according to the literature [24] (Supplemental Material, Fig. S1.a).

The black ink was used to print QR codes version 1 with error correction level L (capacity to correct 7% of damage blocks) and dimensions 3.5 cm × 3.5 cm embedded with text messages "*PHANTOM-G QR CODES*" on transfer paper (*Transfer Paper Inkjet Light* A4), being posteriorly stamped on medical adhesives (*Mefix Molnlyce*) and protection masks (*Polypropylene Particle Filtering Half Mask ORAS-K1*) using a hot iron transfer technique (Fig. 2.a,b). The finder pattern of the QR Code was isolated using an acetate mask, and the dU6Eu ink was airbrushed using an aerograph (*Double Action Airbrush D-102 Dismoer* with a *Mini-Compressor D-15 Dismoer*). The dU6Tb was also printed using a commercial inkjet printer (Brother DCP - J562DW) on paper (Ingres from Fabriano Inc. paper) [24] and superimposed in the medical substrates. The inkjet and airbrush methods allow the generation of a myriad of patterns controlled by the substrate, the viscosity of the ink, the airbrush pressure, the distance of the aerograph to the substrate or the printing velocity, and the number of deposited layers, among others, which makes it an unclonable and unique PUF *response*, suited for authentication. Under daylight illumination, only the regular QR code is visible (Fig. 2.a,b), whereas, under UV illumination, the smart location patterns display a bright red and green color ascribed to the intra-$4f^6$ transitions (Eu^{3+}) and intra-$4f^8$ transitions (Tb^{3+}) excited in the UV/blue spectral range (Fig. 2.c) through efficient ligand-to-Ln^{3+} energy transfer [24], [32]. Selecting the luminescent ink, the white light from the smartphone flashlight may be used as the excitation source. The inks-based emission is typified by a random pattern (Fig. 2.c,d), being the fundamental piece for the exploration of the label as a PUF. The emission color dependence on the excitation wavelength will be used to design a strong PUF that displays distinct *challenge-response* pairs, as detailed below.

C. OPTICAL CHARACTERIZATION

The emission spectra of the univocal labels were measured using a portable spectrometer (OceanOptics Maya 2000 Pro with an integration time of 250 ms, coupled with an optical fiber placed at a central location of the label, under UV lamp excitation (Spectroline ENF-280C/FE). The excitation spectrum was recorded using a modular double grating excitation spectrofluorimeter with an emission monochromator (Fluorolog-3, Horiba Scientific) coupled to a photomultiplier (R928 Hamamatsu), using the front face acquisition mode and was weighed for the spectral distribution of the lamp intensity using a photodiode reference detector.

D. PUF EVALUATION: ACCURACY, PRECISION, AND RECALL

The decisions of an authentication methodology can be True Positives (TP), True Negative (TN), False Positive (FP), and False Negatives (FN). The evaluation metrics was performed through three parameters [38], namely the *accuracy* (Equation 1), that is the percentage of right predictions of the methodology

$$accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \times 100 \tag{1}$$

the *precision* (Equation 2), that is the percentage of correctly predicted Positives on all the predicted positives

$$precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \times 100 \tag{2}$$

and the *recall* that is the percentage of the correctly predicted Positives on all of the real Positives (Equation 3).

$$recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \times 100 \tag{3}$$

All these metrics must be maximized on an authentication methodology.

E. FIGURES OF MERIT FOR OPTICAL SENSING

The figures of merit to evaluate the performance of the thermometers are the relative sensitivity, S_r, and the temperature uncertainty, δT, defined as [39]:

$$S_r = \frac{100}{\Delta} \left| \frac{\partial \Delta}{\partial T} \right| \tag{4}$$

$$\delta T = \frac{1}{S_r} \frac{\delta \Delta}{\Delta} \tag{5}$$

where $\delta\Delta$ is the uncertainty in the determination of the thermometric parameter (Δ). The $\delta\Delta/\Delta$ is the average error of the thermometric parameter (Equation S6).

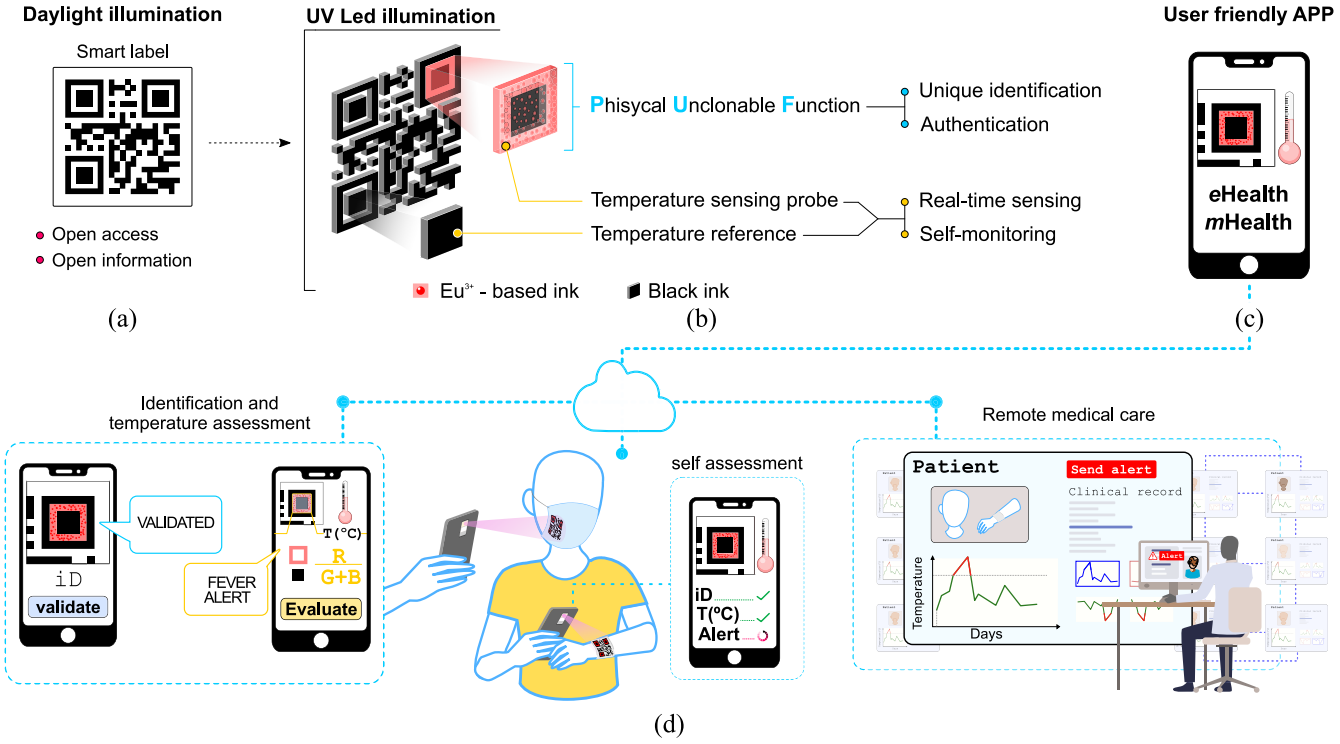


FIGURE 1. Schematic representation of the PUF methodology and the different possible outputs. a) Under daylight illumination only the black/white QR code is visible being used for open access operations. b) Under excitation with a UV LED the dU6Eu material is activated and the Physical Unclonable Function response is revealed. Also, b exploring the dU6Eu color thermal dependence combined with the stable color from the black ink location pattern a temperature sensor is designed. c) Both scenarios are assisted by a smartphone with a user-friendly application (APP) allowing for temperature sensing, label validation, and IoT connection. d) Univocal smart labels produced on medical adhesives and individual protection masks for remote medical care and identification and temperature assessment applications. The concept is also illustrated in the video abstract from the IEEE website.

III. IMPLEMENTATION OF PHYSICAL UNCLONABLE FUNCTION

A. AUTHENTICATION METHODOLOGY

Under UV illumination (*challenge*) the customized QR code displays the randomly distributed emission that will create a PUF *response* detectable using a smartphone photographic record. The acquisition of a photograph is optimized by the presence of the QR code that automatically assists the orientation and alignment of the PUF to acquire the *responses* to the *challenge*. The generic authentication methodology is divided into two main stages, the e*nrollment* and the *verification* [40], [41], Fig. 3.b. The *enrollment* stage starts with the application of the *challenge* to the label and acquisition of smartphone-detectable *response*. Since the analyzed PUF *responses* are image-based *responses*, perceptual hash functions are used to convert the images into fixed-length digital outputs. The hash vectors or values are generated to identify unequivocally the original content [11], [42]. Therefore, the resultant image is subjected to a preprocessing stage, and the hash extraction results in a hash identifier that is saved on a database. On the *verification* stage, a testing label under authentication will be subject to the same *challenge* to acquire the same type of *response*, as the original one on the *enrollment* stage. Then, the extracted hash identifier is compared with the original one stored in the database, through the calculation of the normalized Hamming distance (*nHD*). One of the main aspects of utilizing PUFs in authentication applications is the requirement of a strong PUF, which must display different *challenge-response* pairs to comply with security features [16], [43]. Our proposal is focused on the hardware token (superimposed on the mask) used to identify a fielded device that incorporates the strong PUF and therefore is suitable for authentication applications. Although extra analysis related to authentication lies beyond the scope of the present work, we note that one of the major security drawbacks (e.g., cyber-attacks) related to PUF is "modeling attacks" based on machine learning algorithms that are trained with sets of *challenge-response* pairs, predicting the possible outcome from the PUF, creating a digital clone. Notably, electronic PUFs are much more exposed to this cloning process than optical ones, as it assumes the basic circuit design with only the manufacturing parameters remaining unknown but being possible to predict with machine learning [43]. The accuracy of the process is very effective as only some electronic PUF designs have not been cloned yet [44]. The optical PUF lies on more complex and unpredictable phenomena with the properties of optical signal offering a higher number of possibilities to generate random patterns with multiple *challenge-response* pairs [8].

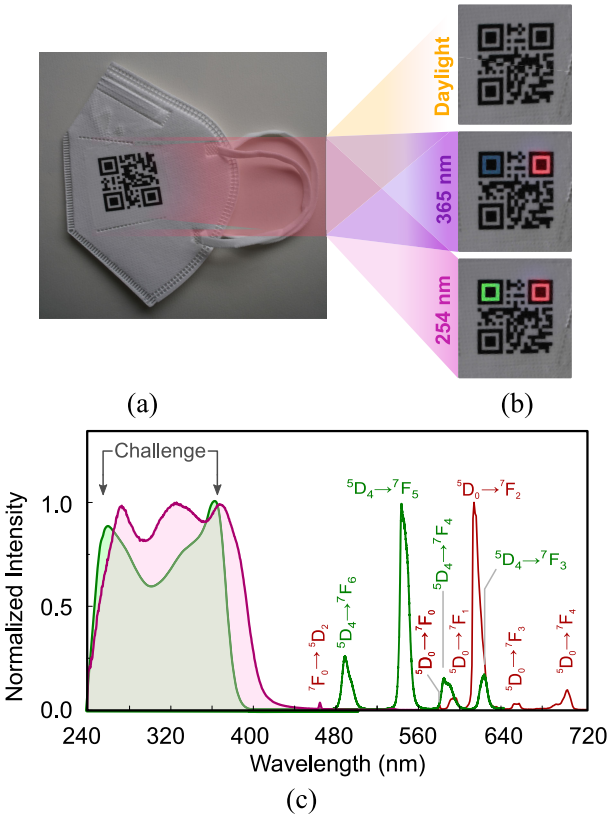


FIGURE 2. Schematic representation of the PUF methodology and the different possible outputs processed in different substrates. Under daylight illumination only the black/white QR code is visible being processed in a) a mask and b) a medical adhesive show under UV LED excitation. c) Excitation and emission spectra monitored at 611/544 nm and excited at 365/254 nm, respectively for dU6Eu/dU6Tb.

B. ACQUISITION AND COMPARISON OF THE RESPONSES

For the acquisition of the *responses*, photographic records of the smart labels were acquired using a commercially available smartphone Xiaomi Mi9 Lite with a resolution of 4000 pixels × 2250 pixels, an aperture of f/1.79, and sensor dimension of 1/2''. To note that the methodology can be applied to every smartphone. Fifteen smartphone photographic records were acquired of a single PUF *response*, varying the distance of the smartphone to the label in the range of 10.0 to 24.0 cm (Fig. 3.c-h and Supplemental Material, Fig. S2.a) and fourteen photographic records of fourteen responses of different PUFs to the same challenge were acquired for a distance of 14.5 cm between the smartphone and the label (Supplemental Material, Fig. S2.b).

The emission of dU6Eu and dU6Tb occurs in the red and green spectral regions, respectively (Fig. 2.c), so the preprocessing of the *responses* is initiated by acquiring the red and green channels from the PUF images, where the relevant information is encoded. The fact that both inks are characterized by pure colors is beneficial as it increases the signal-to-noise ratio and reduces the contribution effects induced by ambient light. To the region of interest (luminescent area), a mean filter with a kernel size of 7 pixels × 7 pixels is applied and that layer is posteriorly resized to 32 pixels × 32 pixels [45]. The chosen perceptual hash procedure to apply on the developed methodologies is the type-II DCT (Discrete Cosine Transform) Hash defined by Equation (6), where N is the size of the real signal sequence where it is being applied [45].

$$c\,[n, m] = \sqrt{\frac{2}{N}} \cos\left(\frac{(2m+1)\,n\pi}{2N}\right), \quad m, n = 0, \ldots, N-1 \tag{6}$$

To apply it on a resultant preprocessed image I, a two-dimensional DCT matrix is calculated programmatically through Equation (7), where c' is the transposed one-dimensional DCT matrix. Then, the most perceptual significant coefficients are extracted from the matrix and converted into a binary form, representing the hash identifiers (Supplemental Material S3, Equation S1). The identifiers are extracted considering only 64 low-frequency hash coefficients, which was observed as a good compromise between key size and effective authentication. The metric that is used to compare different hash identifiers is the *nHD* (Supplemental Material S3, Equation S2) [45].

$$I_{DCT}\,(I) = \mathrm{c} \cdot \mathrm{I} \cdot \mathrm{c}' \tag{7}$$

The acquired hash identifiers of the *responses* are compared with each other, and the resultant values are represented as occurrence histograms fitted to Gaussian probability density functions (*pdfs*). On that representation, there are expected two *pdfs* centered at different values of the normalized Hamming distance. The *pdf* centered at a lower Hamming distance value is assigned to the *responses* of the same PUF acquired at different heights (intra-distances) and the other *pdf* centered on a higher value of Hamming distance is assigned to the comparisons between the responses of different PUFs (inter-distances). The optimal value to separate both distributions (optimum decision level) is obtained by minimizing the probability error function. This optimal value is defined as the threshold used to identify if a PUF is authentic or not, i.e., above the threshold the PUF is not authentic, and below the PUF is validated as authentic (Supplemental Material S4, Equations S3, and S4) [8], [11].

To infer from the robustness of the above-mentioned strategy, the Hamming distances between the responses are represented on a heatmap, from which is possible to verify the occurrence of false predictions. Considering the possible predictions that can result from the authentication, the accuracy, precision, and recall of the methodology are calculated (Equations 1 to 3).

IV. RESULTS AND DISCUSSION

Fig. 2 shows the luminescent univocal smart labels. Under the *challenges* (different excitation wavelengths), a bright red and green emission in the finder patterns is revealed, with visible randomness, forming the PUF smartphone-detectable *response*. The emission color arises from the intra-$4f^6$ (dU6Eu) and intra-$4f^8$ (dU6Tb) transitions excited via

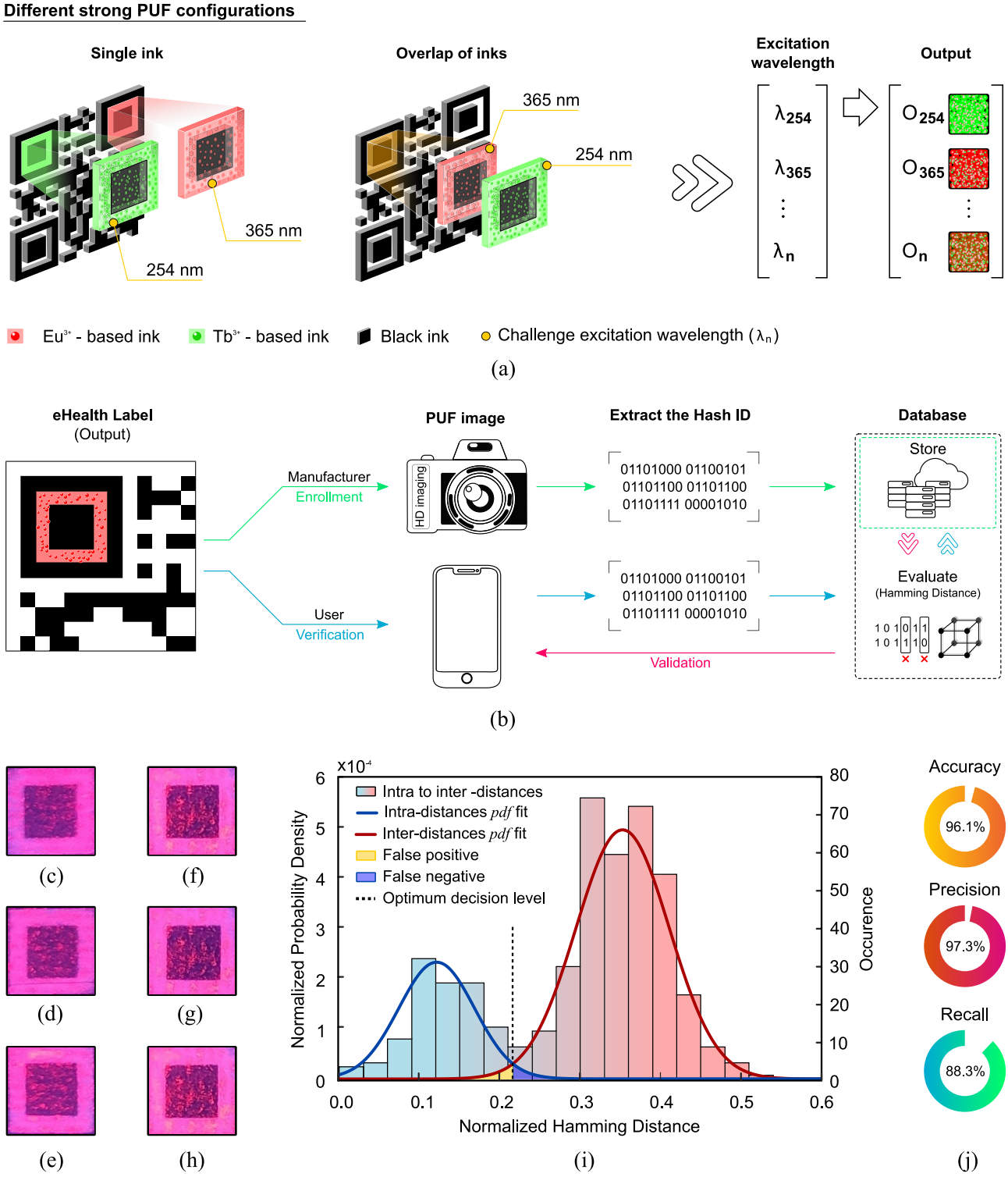


FIGURE 3. a) Schematic representation of the strong PUF creation and evaluation stages. Distinct excitation wavelength (λ_n) yield distinct responses (O_n) b) A PUF is created onto a smart label afterward evaluated by the manufacturer, which starts the enrollment by capturing a high-quality image of the PUF extracting a hash identification string generating a new entrance into a database stored on a server. On the user side, it starts the verification process by capturing an image with a smartphone, extracting the hash identification evaluating it with Hamming distances with the values stored in the database. The process finishes with the user receiving a notification ensuring the validation of the PUF. c-e) Example photographs were taken at 14.5 cm of different generated PUFs. f-h) Example photographs of the same PUF taken at distances 14-16 cm. i) Normalized occurrence histograms and the respective fitting Gaussian pdfs of hamming Distances between all the PUFs responses, showing two Gaussians ascribed to the intra-distances and inter-distances. The optimal decision value of separation of the Gaussian pdfs is also represented, along with the area's representative of the error probabilities. j) Methodology evaluation parameters: accuracy, precision, and recall.

an efficient ligands-to-Eu^{3+}/Tb^{3+} energy transfer [24]. The fact that the ligands absorb mainly in the UV spectral range (Fig. 2.c) confers transparency under daylight and prevents self-absorption due to the high ligands-induced Stokes shift.

All the *responses* were compared with each other through the Hamming distance of the hash identifiers (Fig. S3). Focusing on a single *challenge-response* pair for a selected ink (dU6Eu) the occurrence histograms show two clusters (intra- and inter-distances), allowing their fitting to two *pdfs* (Fig. 3.i). The *pdfs* were weighted attending to the probability of occurrence of each true prediction. The achieved optimal decision value is 0.21 with a probability of a false-positive match of 0.62 % and a false-negative match of 0.52 % (Supplemental Material S5). The obtained few matching errors indicate high reproducibility of the measure of the *responses* of this type of PUF to the same *challenge* and high uniqueness when comparing distinct ones. When establishing this methodology of authentication, is important to notice that the maximum height of the smartphone desirable to acquire the photographs is between 10.0 and 20.0 cm, since above that value, the decreasing of the photographic resolution causes artifacts that influence their comparison. The real values obtained for the false occurrences yield high accuracy, precision, and recall values, Fig. 3.j.

Aiming at strong PUFs, we envisage that the location pattern regions are designed with the dU6Eu and dU6Tb inks enabling different *challenges* (excitation wavelengths) -*response* pairs. For example, the overlap of two distinct layers created with two inks modified with lanthanide ion (Supplemental Information S6) results in the mix of the emission color (Supplemental Material, Fig. S4.b). Once both inks are processed in distinct layers overlapping each other, the mix of the red and green emission colors will occur. The relative intensity of the red (dU6Eu) and green (dU6Tb) color depends on the selected excitation wavelength as the excitation spectra (Fig.2c) point out. For instance, in the lower wavelength range (250 nm) the green is selectively excited, whereas in blue (>400 nm) only the red emission could be discerned. Under selected excitation wavelengths, the *responses* were processed and the DCT hash identifiers were extracted. The normalized Hamming distance is 0.28 which is above the optimal value threshold for the authentication establishing a strong PUF. This methodology opens the possibility to design several *challenge-response* pairs, simply by the judicious choice of the ink. A multitude of inks can be used, playing either with the optical centers or with their concentrations, allowing multiple *challenge-response* pairs.

Besides the use as a PUF, the luminescence from the location pattern was further explored as a luminescent optical sensor, taking advantage of the temperature dependence of the red emission intensity [26], to define a ratiometric luminescent thermometer. As the temperature is raised, there is an increase of the red (R) color coordinate intensity, Fig. 4.a. The color coordinates of the black ink are independent of the temperature and can be used as a reference. The thermometric parameter Δ is defined as the intensity ratio between the red pixel intensity (R) and the black ink green (G) and blue (B) coordinates (Fig. 4.a).

$$\Delta = \frac{R}{G+B} \tag{8}$$

The use of the black ink as reference mitigates possible fluctuations from external factors, increasing the robustness of the temperature readout through a ratiometric thermometric parameter (Fig. 4.b, Supplemental Material, Equations S5-S7).

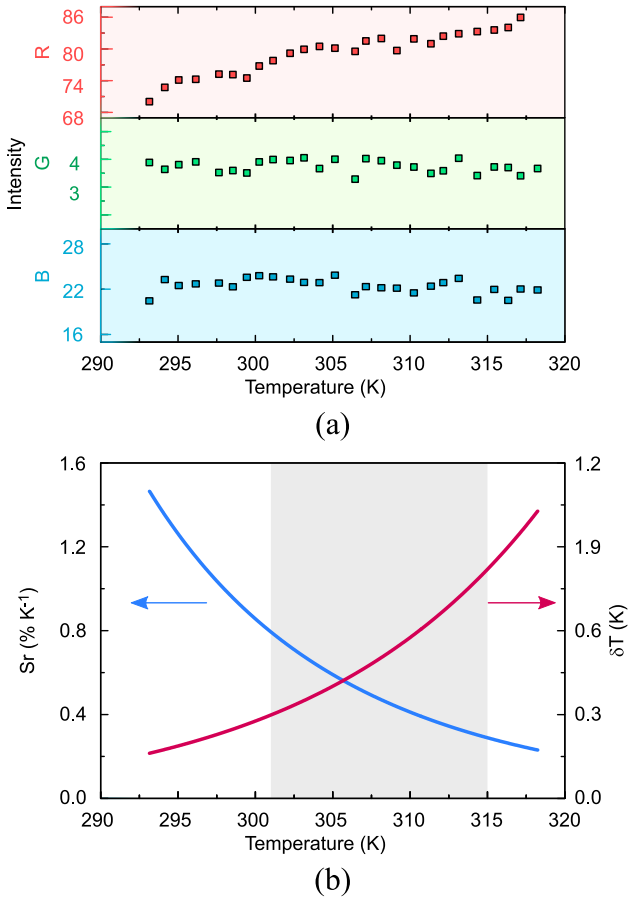


FIGURE 4. a) Color coordinates retrieved from the photographic records as a function of temperature. Thermometer evaluation parameters b) thermal relative sensitivity and temperature uncertainty. The shaded area in b) is the physiological temperature range [48], [49].

The thermometric performance (Equations 4 and 5) [20], yields a maximum relative sensitivity of $S_m = 1.46\ \%K^{-1}$ and minimum temperature uncertainty of $\delta T = 0.2$ K (Fig. 4.b). In the physiological range, the figures of merit are $S_r = 0.41\ \%K^{-1}$ and $\delta T = 0.6$ K, among the best ones in the literature [20], [46], demonstrating the potential of luminescence thermometry for mobile *eHealth* and *mHealth* sensing [26]. We note that such figures of merit are useful to monitor injured or wound body locations, where the temperature variation that may indicate the presence of an infection is usually about 1 °C [47]. Although fever is determined in a shorter temperature range (37.8–40.0 °C), the thermometer here reported is adequate to enable an initial assessment.

V. CONCLUSION

In this work, we demonstrate a univocal smart label incorporated in medical adhesives and masks, based on customized luminescent QR codes with luminescent smart location patterns processed with organic-inorganic hybrid materials doped with lanthanide (Eu^{3+} and Tb^{3+}) complexes. This methodology enables the design of a smart label in which a single QR code is used as an unclonable label able to sense temperature, using a common smartphone. The smartphone provides photographic records and the IoT connection. By exploring the random pattern created by the emission of the overlapped luminescent inks onto the QR code location patterns a strong PUF is created, whose emission color is tunned from green to red (*response*) under distinct UV/blue illumination (*challenge*). High reproducibility of the *response* measures of this type of PUF and their high uniqueness were also demonstrated. For the temperature sensing, a ratiometric thermometer was designed for *eHealth*, endowing the label with more than identification and authentication purposes. It combines two key aspects such as tracking and temperature sensing, having maximum relative sensitivity of 1.46 $\%K^{-1}$, a value within the same order of magnitude as other optical luminescent temperature sensors, and a temperature uncertainty of 0.2 K, inside the threshold needed for *eHealth* applications. Because the processing of the lanthanide-based organic-inorganic hybrids inks is particularly versatile concerning the choice of the ligands and of the lanthanides that can be employed it opens the possibility to control the optical absorption by the judicious choice of the ligands and the emission response that will be set by the selected lanthanide. The present work opens new perspectives for developing a large variety of photoactive inks for smart labels for sensing and to further explore strong PUFs.

ACKNOWLEDGMENT

(Lília M. S. Dias and João F. C. B. Ramalho contributed equally to this work.)

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015, doi: 10.1109/COMST.2015.2444095.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[3] D. Evans, "The Internet of Things: How the next evolution of the internet is changing everything," Cisco, Internet Bus. Solutions Group, San Jose, CA, USA, White Paper, Apr. 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and health: Internet of Things, big data, and cloud computing for healthcare 4.0," *J. Ind. Inf. Integr.*, vol. 18, Jun. 2020, Art. no. 100129, doi: 10.1016/j.jii.2020.100129.

[5] H. H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *J. Netw. Comput. Appl.*, vol. 128, pp. 105–140, Feb. 2019, doi: 10.1016/j.jnca.2018.10.021.

[6] W. B. Arfi, I. B. Nasr, G. Kondrateva, and L. Hikkerova, "The role of trust in intention to use the IoT in eHealth: Application of the modified UTAUT in a consumer context," *Technol. Forecasting Social Change*, vol. 167, Jun. 2021, Art. no. 120688, doi: 10.1016/j.techfore.2021.120688.

[7] I. U. Din, M. Guizani, S. Hassan, B.-S. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019, doi: 10.1109/ACCESS.2018.2886601.

[8] B. T. Bosworth, I. A. Atakhodjaev, M. R. Kossey, B. C. Grubel, D. S. Vresilovic, J. R. Stroud, N. MacFarlane, J. Villalba, N. Dehak, A. B. Cooper, M. A. Foster, and A. C. Foster, "Unclonable photonic keys hardened against machine learning attacks," *APL Photon.*, vol. 5, no. 1, Jan. 2020, Art. no. 010803, doi: 10.1063/1.5100178.

[9] M. Ngan, P. Grother, and K. Hanaoka, "Ongoing face recognition vendor test (FRVT). Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 8311, Jul. 2020, doi: 10.6028/NIST.IR.8311.

[10] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

[11] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *Comput. Netw.*, vol. 183, Dec. 2020, Art. no. 107593, doi: 10.1016/j.comnet.2020.107593.

[12] R. Arppe-Tabbara, M. Tabbara, and T. J. Sørensen, "Versatile and validated optical authentication system based on physical unclonable functions," *ACS Appl. Mater. Interfaces*, vol. 11, no. 6, pp. 6475–6482, Feb. 2019, doi: 10.1021/acsami.8b17403.

[13] Y. Liu, F. Han, F. Li, Y. Zhao, M. Chen, Z. Xu, X. Zheng, H. Hu, J. Yao, T. Guo, W. Lin, Y. Zheng, B. You, P. Liu, Y. Li, and L. Qian, "Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication," *Nature Commun.*, vol. 10, no. 1, p. 2409, Dec. 2019, doi: 10.1038/s41467-019-10406-7.

[14] M. A. Muhal, X. Luo, Z. Mahmood, and A. Ullah, "Physical unclonable function based authentication scheme for smart devices in Internet of Things," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2018, pp. 160–165, doi: 10.1109/SmartIoT.2018.00037.

[15] A. Di Falco, V. Mazzone, A. Cruz, and A. Fratalocchi, "Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips," *Nature Commun.*, vol. 10, no. 1, p. 5827, Dec. 2019, doi: 10.1038/s41467-019-13740-y.

[16] J. Plusquellic, "PUF-based authentication," in *Fundamentals of IP and SoC Security: Design, Verification, and Debug*, S. Bhunia, S. Ray, and S. Sur-Kolay, Eds. Cham, Switzerland: Springer, 2017, pp. 115–166.

[17] M. Akriotou, A. Fragkos, and D. Syvridis, "Photonic physical unclonable functions: From the concept to fully functional device operating in the field," *Proc. SPIE*, vol. 11274, May 2020, Art. no. 112740N, doi: 10.1117/12.2551272.

[18] A. Fratalocchi, A. Fleming, C. Conti, and A. Di Falco, "NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels," *Nanophotonics*, vol. 10, no. 1, pp. 457–464, Oct. 2020, doi: 10.1515/nanoph-2020-0368.

[19] X.-D. Wang, O. S. Wolfbeis, and R. J. Meier, "Luminescent probes and sensors for temperature," *Chem. Soc. Rev.*, vol. 42, no. 19, pp. 7834–7869, 2013, doi: 10.1039/c3cs60102a.

[20] J. F. C. B. Ramalho, L. D. Carlos, P. S. André, and R. A. S. Ferreira, "mOptical sensing for the Internet of Things: A smartphone-controlled platform for temperature monitoring," *Adv. Photon. Res.*, vol. 2, no. 6, Jun. 2021, Art. no. 2000211, doi: 10.1002/adpr.202000211.

[21] K.-D. Gruner, *Principles of Non-Contact Temperature Measurement*. Berlin, Germany: Raytek Company, 2003.

[22] J. F. C. B. Ramalho, A. N. C. Neto, L. D. Carlos, P. S. André, and R. A. S. Ferreira, "Lanthanides for the new generation of optical sensing and Internet of Things," in *Handbook on the Physics and Chemistry of Rare Earths*. Amsterdam, The Netherlands: Elsevier, 2022.

[23] J. F. C. B. Ramalho, S. F. H. Correia, L. Fu, L. L. F. António, C. D. S. Brites, P. S. André, R. A. S. Ferreira, and L. D. Carlos, "Luminescence thermometry on the route of the mobile-based Internet of Things (IoT): How smart QR codes make it real," *Adv. Sci.*, vol. 6, no. 19, Oct. 2019, Art. no. 1900950, doi: 10.1002/advs.201900950.

[24] J. F. C. B. Ramalho, S. F. H. Correia, L. Fu, L. M. S. Dias, P. Adão, P. Mateus, R. A. S. Ferreira, and P. S. André, "Super modules-based active QR codes for smart trackability and IoT: A responsive-banknotes case study," *NPJ Flexible Electron.*, vol. 4, no. 1, p. 11, Dec. 2020, doi: 10.1038/s41528-020-0073-1.

[25] R. A. S. Ferreira, P. S. André, J. F. C. B. Ramalho, and L. D. Carlos, "Multiplexed luminescent QR codes for smart labelling, for measuring physical parameters and real-time traceability and authentication," WO Patent 2021 001 767 A1, Jan. 7, 2020.
[26] J. F. C. B. Ramalho, L. M. S. Dias, L. Fu, A. M. P. Botas, L. D. Carlos, A. N. C. Neto, P. S. André, and R. A. S. Ferreira, "Customized luminescent multiplexed quick-response codes as reliable temperature mobile optical sensors for eHealth and Internet of Things," *Adv. Photon. Res.*, Nov. 2021, Art. no. 2100206, doi: 10.1002/adpr.202100206.
[27] I. Meazzini, S. Comby, K. D. Richards, A. M. Withers, F.-X. Turquet, J. E. Houston, R. M. Owens, and R. C. Evans, "Synthesis and characterisation of biocompatible organic–inorganic core–shell nanocomposite particles based on ureasils," *J. Mater. Chem. B*, vol. 8, no. 22, pp. 4908–4916, Jun. 2020, doi: 10.1039/D0TB00100G.
[28] V. de Zea Bermudez, L. D. Carlos, and L. Alcácer, "Sol–gel derived urea cross-linked organically modified silicates. 1. Room temperature mid-infrared spectra," *Chem. Mater.*, vol. 11, no. 3, pp. 569–580, Mar. 1999, doi: 10.1021/cm980372v.
[29] L. D. Carlos, V. de Zea Bermudez, R. A. Sá Ferreira, L. Marques, and M. Assunção, "Sol–gel derived urea cross-linked organically modified silicates. 2. Blue-light emission," *Chem. Mater.*, vol. 11, no. 3, pp. 581–588, Mar. 1999, doi: 10.1021/cm980373n.
[30] C. Molina, K. Dahmouche, Y. Messaddeq, S. J. L. Ribeiro, M. A. P. Silva, V. de Zea Bermudez, and L. D. Carlos, "Enhanced emission from Eu(III) β-diketone complex combined with ether-type oxygen atoms of di-ureasil organic–inorganic hybrids," *J. Lumin.*, vol. 104, nos. 1–2, pp. 93–101, Jun. 2003, doi: 10.1016/S0022-2313(02)00684-1.
[31] M. Fernandes, V. de Zea Bermudez, R. A. S. Ferreira, L. D. Carlos, A. Charas, J. Morgado, M. M. Silva, and M. J. Smith, "Highly photostable luminescent poly(ε-caprolactone)siloxane biohybrids doped with europium complexes," *Chem. Mater.*, vol. 19, no. 16, pp. 3892–3901, Aug. 2007, doi: 10.1021/cm062832n.
[32] M. Fang, A. G. Bispo-Jr, L. Fu, R. A. S. Ferreira, and L. D. Carlos, "Efficient green-emitting Tb^{3+}-doped di-ureasil coating phosphors for near-UV excited light-emitting diodes," *J. Lumin.*, vol. 219, Mar. 2020, Art. no. 116910, doi: 10.1016/j.jlumin.2019.116910.
[33] S. F. H. Correia, P. P. Lima, P. S. André, M. R. S. Ferreira, and L. A. D. Carlos, "High-efficiency luminescent solar concentrators for flexible waveguiding photovoltaics," *Sol. Energy Mater. Sol. Cells*, vol. 138, pp. 51–57, Jul. 2015, doi: 10.1016/j.solmat.2015.02.032.
[34] P. P. Lima, R. A. Sá Ferreira, R. O. Freire, F. A. Almeida Paz, L. Fu, S. Alves, L. D. Carlos, and O. L. Malta, "Spectroscopic study of a UV-photostable organic-inorganic hybrids incorporating an Eu^{3+} β-diketonate complex," *ChemPhysChem*, vol. 7, no. 3, pp. 735–746, Mar. 2006, doi: 10.1002/cphc.200500588.
[35] L. D. Carlos, R. A. S. Ferreira, V. D. Z. Bermudez, and S. J. L. Ribeiro, "Lanthanide-containing light-emitting organic-inorganic hybrids: A bet on the future," *Adv. Mater.*, vol. 21, no. 5, pp. 509–534, Feb. 2009, doi: 10.1002/adma.200801635.
[36] P. P. Lima, M. M. Nolasco, F. A. A. Paz, R. A. S. Ferreira, R. L. Longo, O. L. Malta, and L. D. Carlos, "Photo–click chemistry to design highly efficient lanthanide β-diketonate complexes stable under UV irradiation," *Chem. Mater.*, vol. 25, no. 4, pp. 586–598, Feb. 2013, doi: 10.1021/cm303776x.
[37] T. A. Popov, T. Z. Kralimarkova, and V. D. Dimitrov, "Measurement of exhaled breath temperature in science and clinical practice," *Breathe*, vol. 8, no. 3, pp. 186–192, Mar. 2012, doi: 10.1183/20734735.021811.
[38] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in Internet of Things environment," *Comput. Commun.*, vol. 163, pp. 109–133, Nov. 2020, doi: 10.1016/j.comcom.2020.09.006.
[39] C. D. S. Brites, A. Millán, and L. D. Carlos, "Lanthanides in luminescent thermometry," in *Handbook on the Physics and Chemistry of Rare Earths*, vol. 49, J.-C. Bünzli and V. K. Pecharsky, Eds. Amsterdam, The Netherlands: Elsevier, 2016, pp. 339–427.
[40] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security: Foundations and Practice*, A.-R. Sadeghi and D. Naccache, Eds. Berlin, Germany: Springer, 2010, pp. 3–37.
[41] A. Babaei and G. Schiele, "Physical unclonable functions in the Internet of Things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, Jul. 2019, doi: 10.3390/s19143208.
[42] Y. Saez, C. Estebanez, D. Quintana, and P. Isasi, "Evolutionary hash functions for specific domains," *Appl. Soft Comput.*, vol. 78, pp. 58–69, May 2019, doi: 10.1016/j.asoc.2019.02.014.
[43] F. Pavanello, I. O'Connor, U. Ruhrmair, A. C. Foster, and D. Syvridis, "Recent advances in photonic physical unclonable functions," in *Proc. IEEE Eur. Test Symp. (ETS)*, May 2021, pp. 1–10, doi: 10.1109/ETS50041.2021.9465434.
[44] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Ü. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 237–249, doi: 10.1145/1866307.1866335.
[45] C. Zauner, "Implementation and benchmarking of perceptual image hash functions," M.S. thesis, Univ. Appl. Sci. Upper Austria, Wels, Austria, 2010, pp. 4–30.
[46] C. D. S. Brites, S. Balabhadra, and L. D. Carlos, "Lanthanide-based thermometers: At the cutting-edge of luminescence thermometry," *Adv. Opt. Mater.*, vol. 7, no. 5, Mar. 2019, Art. no. 1801239, doi: 10.1002/adom.201801239.
[47] M. S. Brown, B. Ashley, and A. Koh, "Wearable technology for chronic wound monitoring: Current dressings, advancements, and future prospects," *Frontiers Bioeng. Biotechnol.*, vol. 6, p. 47, Apr. 2018, doi: 10.3389/fbioe.2018.00047.
[48] J. Kuht and A. D. Farmery, "Body temperature and its regulation," *Anaesthesia Intensive Care Med.*, vol. 19, no. 9, pp. 507–512, Sep. 2018, doi: 10.1016/j.mpaic.2018.06.003.
[49] J. Kuht and A. D. Farmery, "Body temperature and its regulation," *Anaesthesia Intensive Care Med.*, vol. 15, no. 6, pp. 273–278, Jun. 2014, doi: 10.1016/j.mpaic.2014.03.013.

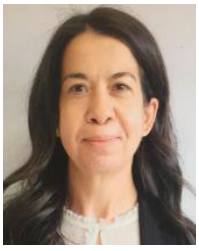
LÍLIA M. S. DIAS received the M.Sc. degree in biomedical engineering from the University of Aveiro, Aveiro, Portugal, in 2021, with her major field of study on luminescent smart labeling for Internet of Things, temperature sensing and authentication on healthcare applications. Her research interests include optical sensing, authentication, and smart labeling.

JOÃO F. C. B. RAMALHO received the Ph.D. degree in physics engineering from the University of Aveiro, in 2022.

He was a Research Fellow with the CICECO—Aveiro Institute of Materials, from 2016 to 2022, working in the field of photonics and materials engineering, developing research on luminescent smart labels for the new generation of optical sensing and the Internet of Things. His research interests include the fields of smart labeling, the Internet of Things, optical sensing, and luminescent thermometry.

TIAGO SILVÉRIO received the M.Sc. degree in physics engineering from the University of Aveiro, Aveiro, Portugal, in 2021, while working on physically unclonable functions towards object authentication and identification. His research interests include the simulation and implementation of visible light communication systems.

LIANSHE FU received the Ph.D. degree in chemistry from the Changchun Institute of Applied Chemistry, Chinese Academy of Sciences, China, in 1999. Since 2007, he has been a full-time Researcher with the Department of Physics, Department of Chemistry, CICECO—Aveiro Institute of Materials, University of Aveiro, Portugal. His current research interests include lanthanide- and carbon dots-based organic-inorganic hybrids for functional materials and their applications in optoelectronic and photonic devices.



RUTE A. S. FERREIRA received the Ph.D. degree in physics, in 2002, and the Agregação (Habilitation) degree in physics from the Universidade de Aveiro (UA), Portugal. She is currently an Associate Professor with the Department of Physics, UA. She is also the Vice-Director of the CICECO—Aveiro Institute of Materials and a member of the General Board of UA. Her current research interests include the optoelectronic studies of organic/inorganic hybrids foreseeing applications in the fields of optoelectronics and green photonics (solid-state lighting and integrated optics) and photovoltaics (luminescent solar concentrators and down-shifting layers).

PAULO S. ANDRÉ (Senior Member, IEEE) received the bachelor's degree in physics engineering, in 1996, the Ph.D. degree in physics, in 2002, and the Agregação (Habilitation) degree in physics from the Universidade de Aveiro, Portugal. He is currently a Full Professor with the Department of Electrical and Computer Engineering, Instituto Superior Técnico (IST), University of Lisbon. He is also a Senior Researcher with the Instituto de Telecomunicações. His current research interests include the study and simulation of photonic and optoelectronic components and systems for telecommunication, sensing, and energy applications.