Cholesteric Spherical Reflectors as Physical Unclonable Identifiers in Anti-counterfeiting

Monica P. ARENAS
SnT/University of Luxembourg
Luxembourg
monica.arenas@uni.lu

Huseyin DEMIRCI
SnT/University of Luxembourg
Luxembourg
huseyin.demirci@uni.lu

Gabriele LENZINI
SnT/University of Luxembourg
Luxembourg
gabriele.lenzini@uni.lu

ABSTRACT

Cholesteric Spherical Reflectors (CSRs) are made of droplets of cholesteric liquid crystals (the same material under the screen of our mobile phones) but molded in a spherical shape and hardened into a solid. CSRs have a peculiar behavior when illuminated: they reflect light and produce unique optical patterns whose full display is hardly predictable. They have been argued to behave like an optical Physical Unclonable Function (PUF), therefore finding application in anti-counterfeiting, in particular for object authentication. However, a fundamental challenge remains open: to understand what makes each optical response unique and how to extract this identifying information reliably and repeatedly. We study the problem, and we design and discuss two pivotal procedures to build authentication protocols for objects coated with CSRs. We test the quality of our procedures against large data sets of pattern images: images from CSRs are used to calculate inter- and intra-distance; simulated patterns created artificially are used to measure security in terms of false positive ratio. Our procedures successfully cluster images coming from the same CSR, distinguishing them from images of different CSRs and decoys. Our work is one of the few that has studied procedures of information extraction for materials derived from CSRs. It advances the state of the art in this area, closing the gap between the research on optical PUFs and practical applications.

CCS CONCEPTS

• **Security and privacy** → **Authentication**; **Access control**.

KEYWORDS

Physical unclonable function, authentication, anti-counterfeiting Cholesteric Spherical Reflectors

ACM Reference Format:
Monica P. ARENAS, Huseyin DEMIRCI, and Gabriele LENZINI. 2021. Cholesteric Spherical Reflectors as Physical Unclonable Identifiers in Anti-counterfeiting. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, Article 4, 11 pages. https://doi.org/10.1145/3465481.3465766

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08.
https://doi.org/10.1145/3465481.3465766

1 INTRODUCTION

To check whether a good (*e.g.,* artworks, luxury objects, spare parts, drugs) is original, the good should carry some inimitable features that make it clearly distinguishable from fakes and imitations. This is what tamper-evident seals, special coatings, brand-carrying marks applied or hidden in the originals and easily verifiable by eye or with the help of simple machines are supposed to achieve.

With the right technology and know-how, however, such measures can be replicated well enough to fool a human verifier. Strong anti-counterfeiting elements must therefore be unclonable, and their uniqueness and integrity verifiable without ambiguity. Novel materials are constantly proposed for this purpose, for instance, microscopic particles or special inks that, when applied or sprayed on packages, leave non-reproducible detectable spots with UV light, IR laser, or magnetic field (*e.g.,* see [6, 22, 29]). QR codes or RFIDs can be added to provide identifiers with higher security guarantees and to enable track-and-trace (*e.g.,* see [28]).

Particularly demanded in this business are materials that behave as Physical Unclonable Functions (PUFs) (*e.g.,* just a matter for example since the literature on PUFs for anti-counterfeiting is extremely large, see [3, 4, 12, 16, 18]). They respond to a certain set of stimuli as if they were one-way functions. The responses cannot be reproduced since a PUF is physically unclonable. Existing PUFs are quite different from one another and offer varying guarantees of security, for instance, robustness, unsimulability, unpredictability (*e.g.,* see the survey on PUFs [14]). Their applicability in a specific market sector depends on their nature (*e.g.,* electronic, optical, magnetic, etc.) and here we are interested in those which are *optical*: they respond to light and this response can be captured by a digital camera. Once rare, optical PUFs are becoming common but for each of them remains the problem of determining what identifying information is contained in their responses, how to extract it, and how to use it in a secure authentication procedure. The material and its readout and information extraction procedures constitute a *PUF System* [1] whose robustness, reliability, and security have to be assessed to rightly decide for which anti-counterfeiting sector the system is more suitable: more expensive goods require stronger guarantees [4].

We study these issues and propose solutions for a relatively new optical PUF: spherical droplets of cholesteric liquid crystals hardened into a solid, called *Cholesteric Spherical Reflectors (CSRs).* Arrays of them can be incorporated in a transparent tag[1] as the one in Figure 1-a. Each array of CSRs in unclonable. When illuminated, CSRs produce peculiar optical patterns detectable in visible and/or

[1] CSRs can be also dispersed into a coating, for instance, a transparent nail polish, but how to apply CSRs is not relevant in the scope of this paper, although it makes the difference in terms of marketing applicability.

invisible spectra [8] which have been argued to be unique and hardly replicable [12] and, for this reason, suggested as a technology for anti-counterfeiting [9, 16, 20].

2 BACKGROUND AND STATE OF THE ART

This work relates to previous research on PUF, in particular to optical PUFs. PUF-based technologies exist in great variety, *e.g.,* there are silicon-, chemical-, magnetic-, and optical-based constructions, to cite a few. Making a full account goes beyond our scope but recent surveys could give a broad overview of existing technologies [16].

While most of the PUF (*e.g.,* silicon-based) are embedded into their hosts at the fabrication process—they are called *intrinsic*—*optical* PUFs are not. They are categorized as *non-intrinsic* and have the advantage of being externally observable [14]. They find a natural application in anti-counterfeiting since Pappu et al. [18] introduced the concept of optical PUFs as a *physical one-way function.* They proposed the use of tokens composed of particles randomly distributed on a transparent surface which produce a highly random and unpredictable response when interacting with emitted light (*e.g.,* laser). Due to the unique patterns obtained through complex interactions between light and particles, other authors have proposed optical PUFs under different constructions [3, 4, 8, 9, 12, 16].

CSR tags emerged as potential optical PUFs due to the diverse and unpredictable responses in different wavelengths, ranging from infrared, passing through the visible light until the ultraviolet spectrum, which allows use cases in a variety of applications. One of the potential applications is in anti-counterfeiting technologies, in which the read-out can be smartphone cameras (for overt tags) or low-cost optical components for reading covert tags; but other applications have been proposed, *e.g.,* for robot navigation and in relation to digital twin models [19].

A single CSR tag can generate a wide set of responses that depend on the wavelength, incidence angle, and illumination conditions. The raw materials used in CSR tag production have low costs, allowing to produce a massive amount of tags at affordable prices. The large information coding capacity of CSR tag enables to label a large number of different objects and potentially to identify one from another. There is only one work that attempted to quantify the intra- or inter-distance, giving first evidence that responses from CSR tags can be distinguished [12]. The present work advances that preliminary research with more efficient algorithms, larger data sets and experiments, and far better results, as shown in Section 5.1. It improves the know-how about CSRs and their use in object identification and anti-counterfeiting.

2.1 CSRs in a Nutshell

Details about the material science aspects of CSRs are given in [9]. Here we recall the essential facts relevant in this work. The liquid crystal molecules in a CSR are spontaneously organized in a helical arrangement, with the helix axis along the sphere's radius. The interactions between the incident light and the CSR arrays thus render intricate colorful patterns, the features of which depend on the properties of the CSRs, their arrangements, as well as the illumination and viewing conditions [9]. The selective reflection coming from CSRs can be controlled by adjusting the chemical composition of the liquid crystals, and so can be the size of the droplets during the production process; but the positions of CSRs and the distribution of different CSR types, optimized for main reflections in different parts of the spectrum, *e.g.,* for red (R), green (G) and blue (B), are uncontrollable factors.

Figure 1 (b-d) shows examples of patterns photographed under different illumination conditions with a USB Dino-Lite digital microscope over a CSR's sample. In Figure 1-b, taken with the 4 LEDs of the microscope switched on, the patterns show red spots as many as the active LEDs and blue- and red-reflecting patterns due to the photonic cross-communication between the neighbor shells [17, 20]. Figure 1-c shows the response with 8 LEDs switched on, whereas Figure 1-d is the response with an external lateral illumination.

3 DEFINITION AND REQUIREMENTS

The problem of using a material to tag an object, say i, for the purpose of anti-counterfeiting, is subsumed into an apparently simple authentication problem. Let us call w_i object i tagged with w. When Alice acquires a tagged object w claimed to be the original i and wishes verify that $w == w_i$ (here'==' denotes physical identity), she has to probe w, reading out from it some piece of identifying information, $t = \mathsf{ReadOut}[w]$. In case of a tag made of CSRs (let us call it, a *CSR tag*), the t will be a picture of the tag's optical response as one of those reported in Figure 2. To verify w's originality, Alice has also to process t to extract some unique identifying feature, say z, that is $z = \mathsf{Extract}[t]$. For instance, z can be obtained by applying Gabor filters [25], fuzzy extractors [7], or some feature extraction methods (*e.g.,* see [11]). Then, Alice authenticates w by retrieving the safely stored $z_i = \mathsf{Extract}[\mathsf{ReadOut}[w_i]]$ of the original object and by comparing against it her z. Figure 2, adapted from [2] and from [12], visualizes the workflow and its steps, where $\mathsf{IsMatching}[z, z_i]$ is the final matching test[2].

A full authentication protocol will be more elaborated than just matching z and z_i, but disregarding this aspect at the moment, to solve which we can refer to the literature in PUFs and biometric authentication (*e.g.,* see [5]), what matters is that the robustness and security of the authentication procedure depends on w, on the readout/extraction procedures, and on the algorithm used for the matching. These procedures should be designed, implemented, and combined to satisfy that $\mathsf{IsMatching}[z, z_i] \iff (w == w_i)$.

When w is a PUF, as it is for a CSR tag, each reading out depends on a challenge $x \in \mathbf{X}$, that is $t(x) = \mathsf{ReadOut}[w(x)]$. The PUF system should then satisfy the following requirement:

$$\forall x \in \mathbf{X} : \mathsf{IsMatching}[z(x), z_i(x)] \iff (w == w_i) \qquad (1)$$

3.1 Reliability, Robustness, and Security

In practice, assessing whether requirement (1) holds for a certain PUF system design has to be quantified experimentally and requires the availability of a large set of golden data made of different productions and readouts. This is necessary even if there is a vast literature on image processing and information extraction for PUFs

[2] The figure shows also the process for the production of CSRs: here, parameters α can enhance the entropy carried by a CSR, for instance by varying the density, size, and polarization of the droplets.

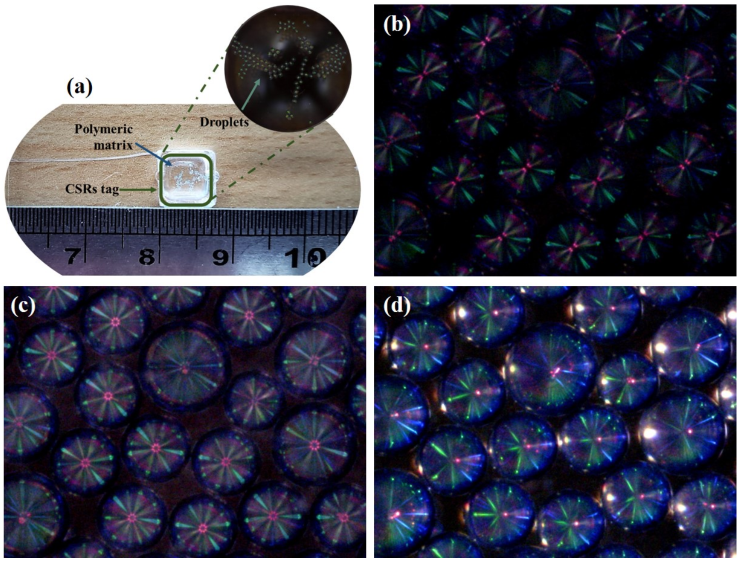


Figure 1: (a) Overview of a $7\times7\times2$ *mm* CSR tag. Optical images of CSRs taken in the same area under different illumination conditions with a USB Dino-Lite digital microscope with a perpendicular illumination to the sample with (b) 4 LEDs illumination; (c) 8 LEDs illumination; (d) illumination with an external source non-perpendicular to the sample.

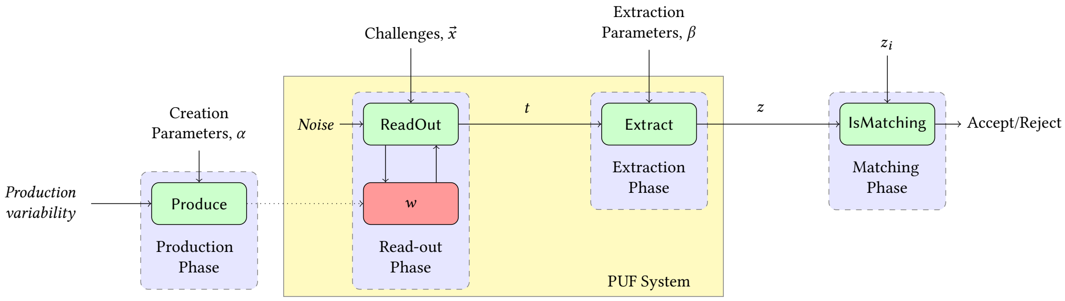


Figure 2: Readout, Extraction and Matching: three phases for object authentication relying on PUF-like coating or tags.

(*e.g.,* see [14]) because any material is different and has its own physical features, different responses, and ways to be analyzed.

Robustness. A robust authentication process should, for a specific CSR tag, accept any image of an optical response of that tag, *despite the inevitable presence of noise* during the readout. In fact, any *retake* (*i.e.,* any optical response taken from the same tag in another moment in time) is quite likely not the same because of the presence of, for instance, different ambient light and position of the physical tag under the camera. If $t_0 = \text{ReadOut}[w_0(x)]$ is a reference readout of w_0, if $t' = \text{ReadOut}'[w_0(x)]$ is any retake of w_0, and if $z'(x) = \text{Extract}[\text{ReadOut}'[w_0(x)]]$ is the corresponding identifying information, then robustness is formalized as follows:

Definition 3.1 (Robustness).

$$(w == w_i) \Rightarrow \forall x \in \mathbf{X} \ \wedge \ \forall z'(x) : \text{IsMatching}[z'(x), z_0(x)] \quad (2)$$

As we will see in the next section, robustness is assessed in terms of false negative ratio and intra-distance between a reference readout and all its retakes. We stress that Definition 3.1 does not suggest how to implement Extract or IsMatching. However, it suggests that the chosen implementation should work for all the different challenges x, *i.e.,* it should be independent of any specific x. This is advisable: we do not wish to have a family of Extract and IsMatching each for a different x. It would be impractical because of the great number of conditions in $\mathbf{X}$ (*e.g.,* size, polarization, number, and density of droplets, angle of readout). A CSR tag can respond differently to each of them. We also seek for an implementation that is as much as possible independent from readout settings (*e.g.,* type of microscope, magnification of the readout), because this is what we expect in realistic anti-counterfeiting scenarios. Figure 3 shows the variability of the readout images for the CSR tags we used in our experiments.

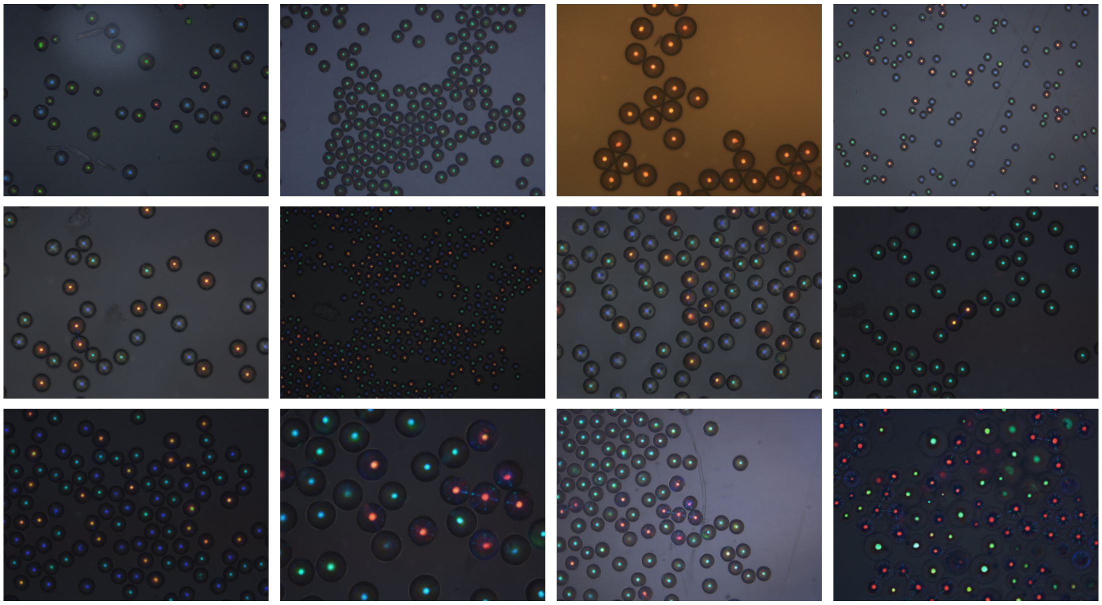


Figure 3: The set of images that we have from our CSR tags, showing great variability in the Read-out Phase.

Reliability. A PUF system for CSRs should also be reliable. Meaning that it should reject any other image of responses generated by any other CSR tag.

Definition 3.2 (Reliability).

$$w \neq w_i \Rightarrow \forall x \in \mathbf{X} \wedge \forall z'(x) : \neg(\mathsf{IsMatching}[z'(x), z_0(x)]) \quad (3)$$

We will measure reliability in terms of false positive ratio and inter-distance between readout from a CSR tag and the set of retakes from other CSR tags.

Security. Secure extraction and matching algorithms should distinguish and reject images that are not taken from any real CSR tag, for instance images that have been artificially constructed. We will measure the security in terms of false positive ratio and inter-distance between readout from a CSR tag and a set of fake readout images that we have artificially and systematically generated.

3.2 Algorithms Design

We discuss two algorithm designs for our Extract and IsMatching: *Image Subtraction* and *Blob Extraction.*

Image Subtraction. This design compares two images directly, without extracting any particular feature from them. Extract does not change the readout, while IsMatching will process the images and compare them taking into account that even if w is authentic (*i.e.,* any $t(x)$ is a retake of the original $w_0(x)$) there will be noise. That is, $t(x)$ can be, with respect to $w_0(x)$, blurred, rotated, shifted, slightly magnified, or affected by other variations, *e.g.,* different background colour due to ambient light and the illumination from the microscope. The noise has to be removed, and $t(x)$ and $t_0(x)$ must be aligned.

Two aligned images are subtracted one from the other, and the *Image Subtraction score* is calculated as the ratio between the number of zeroed pixels over the number of all pixels. Section 4.2 describes the implementation of this design idea.

Blob Extraction. This second design is inspired by a technique that is called *minutiæ detection*, in fingerprint analysis, or *feature extraction* in general biometric analysis (*e.g.,* [27]). The technique consists in extracting from an image specific elements that are argued to be identifying features.

What are those features and minutiæ in a CSR tag's response? CSRs droplets are spherical so their center is a concept geometrically well defined. In a CSR tag's response, centers reflect light, *i.e.,* observation along the direction of illumination yields a circular reflection spot at the center of every CSR. These colored elements are present across all different responses. There are also other colored features in the patterns, with certain radial and azimuthal distributions in reference to the centers of each CSR. They are visible on some images in Figure 3 and in Figure 1-(b-d).

These observations suggest that we can consider as primaries minutiæ the colored circles of different sizes and position that can be recognized in a response taken from a CSR tag. Some minutiæ will be aligned with a droplet physical center, others will have a specific geometrical relationship with the overall arrangement of CSRs within the tag. We call these primaries minutiæ *blobs* and they can be detected with customized techniques of image processing. In addition, the colors generated by CSR droplets due to their "cross-communication" constitute a secondary set of minutiæ. Some of them also have blob-like shape[3].

[3] Our current implementation works with these secondary minutiae when they produce blob-shaped color spots (see image in column 2 row 3 in Figure 3). Some cross-communications, instead, are colored segments. Considering them in the matching, as well as extracting them, is future work.

We stress that here we analyze the minutiæ/blobs in images obtained from a single challenge-response combination. Significantly, this procedure must be repeated for *multiple* images, corresponding to difference challenges, and different responses from the CSR tag to exploit the PUF-characteristics of CSR-based authentication. While we thus do not fully probe the PUF aspects of the tags in this paper, the procedures that we develop here will form the basic algorithmic building blocks for the full implementation of CSR tag authentication.

In Section 4.2, we describe the implementation for Extract and IsMatching of this design idea. The matching relies on a *Blob Extraction score* built as follows: let $\mathsf{Blobs}[t(x)] = \{b_1, \cdots, b_k\}$ be a list of blobs extracted from a read-out $t(x)$, and b.circle and b.color be, respectively, the circle (*i.e.,* centre position and radius) of b and its colour *e.g.,* in RGB.

We call $\bar{t}(x)$ the processed version of t which has been aligned with $t_0(x)$. Our implementation of *Blob Extraction score* depends on an equivalence relation, $=_b$ that defines when two blobs do match according to the relative positions of their circles and their colours. Using them, we can construct *local matching structures* [10, 15], $\mathsf{MatchingBlobs}[\bar{t}(x), t_0(x)]$ as the set of minutiæ in $\mathsf{Blobs}[\bar{t}(x)]$ and $\mathsf{Blobs}[t_0(x)]$ in relation with one another according to $=_b$. After the image alignment, given a local structure, we can calculate a *global matching score* (*i.e.,* our Blob Extraction score) as follows:

$$\frac{2 \times |\mathsf{MatchingBlobs}[\bar{t}(x); t_0(x)]|}{|\mathsf{Blobs}[\bar{t}(x)]| + |\mathsf{Blobs}[t_0(x)]} \tag{4}$$

Whether IsMatching will depend on this score. More elaborated scores will be studied in future work.

4 MATERIALS AND METHODS

4.1 Data Set

We used an extensive number of read-outs in this research: *12 reference images* taken from 12 *physical CSR tags*; 4800 *retake images* simulating different conditions of noise during retake, the benchmark set for our implementation; 2000 *additional retake images*, for validation of robustness and reliability; 1000 *fake CSR tag's readout images*, for the evaluation of security. Data sets are explained below.

Physical CSR tags. We used 12 tags which CSRs have a diameter ranging from 50 μm, to 100 μm coming from different productions. These CSR tags were given by the Experimental Soft Matter Physics (ESMP) group, from the Department of Physics and Materials Science at the University of Luxembourg. Producing a CSR tag is still a time-consuming process, so 12 is indeed a reasonable number of tags to work with.

Reference images. From each CSR tag an optical image was acquired with a polarizing microscope and assumed as the reference image. In total, 12 reference images were used in this manuscript, in our notation $t_1(x), \ldots, t_{12}(x)$. The images were acquired with an optical microscope, equipped with a digital camera and illumination perpendicular to the sample. The reference images were taken by the ESMP group and for simplicity we kept the same labels as provided by them: `Img228`, `Img618`, `Img852`, `Img972`, `Img974`, `Img975`, `Img997`, `Img1060`, `Img1079`, `Img1103` , `Img1104`, and `Img2366`.

Retakes images for testing and tuning. In a real scenario, a retake image of a CSR tag response is affected by noise factors such as positioning a tag under the camera, lighting conditions, magnification, and poor focus. Robust evaluation methods are required to work under such noise-affected imaging conditions.

We created a set of noisy retakes by applying to the reference images the operations listed in Table 1. Each of the 12 reference images was resized, rotated[4], and blurred to simulate various end-user factors such as tag positioning, lighting conditions, and out-of-focus images. The rationale of our choices for 'Range' as in Table 1 is to keep the noise within realistic conditions of a user reading out from a CSR tag. Our choice of range in resizing and rotating simulate reasonable differences in positioning a tag under the camera, while blurring simulates images that are reasonably out-of-focus. This blurring limited up to a 5 × 5 pixel window. This is still considerable noise, capable of making fail image recognition in artificial intelligence[5].

Figure 4-(b) shows one of the mutated images which was resized 110%, rotated 10° anticlockwise and blurred (this latter not fully appreciated due to the low definition of the printed picture). Figure 5 shows the effect of noise on our Image Subtraction score when we consider larger ranges of noise: blur is the only noise that is capable of great disruption, as expected. From an engineering viewpoint, we can attempt to control the noise operating on the readout setting, for instance, by using a special holder for positioning the tag, patterns drawn on the tag for image alignment like those we find in QR codes, and auto-focus cameras.

Note: Simulating possible noise is a standard procedure since it would be an extremely time-consuming and quite uncontrollable strategy to generate noise by hand. We tried for instance to switch on and off the light, to slightly move a CSR tag under the microscope, to remove and re-position a CSR tag. The produced images were not different from those we have obtained by simulating the noise directly by image manipulation. In this latter case, we have the advantage of a finer control over the noise (*e.g.,* in the angle of rotation), and the ability to create a large number of images: for each of the 12 reference images, we generated 400 retakes, for a total of 4800 retakes. This number would have been hardly achievable if we had taken the images by hand.

Table 1: Operations applied to each reference image for obtaining the set of mutated images.

Sequence	Operation	Range
1	Resizing	101 − 110%
2,3	Rotation	1 − 10° (anticlockwise/clockwise)
4	Blurring	(2 × 2) − (5 × 5)

Fake CSR tag's readout images. We generated 1000 *simulated images* of response. They are meant to represent the responses of unauthentic tags, or tampered images of responses. This set is generated from three "seeds" of 3-colored blobs, copied, and pasted

[4] The function was `imutils.rotate`, which rotates the center of the image according to the number of angle degrees. However, for non-squared images, this function crops the edges of the image: thus, rotation is actually rotation and cropping.

[5] For instance, a 5 × 5 pixel window blurring fools Wolfram Language's AI to identify an image of a tiger as a fish: `ImageIdentify[Blur[=tiger["Image"],5]]`.

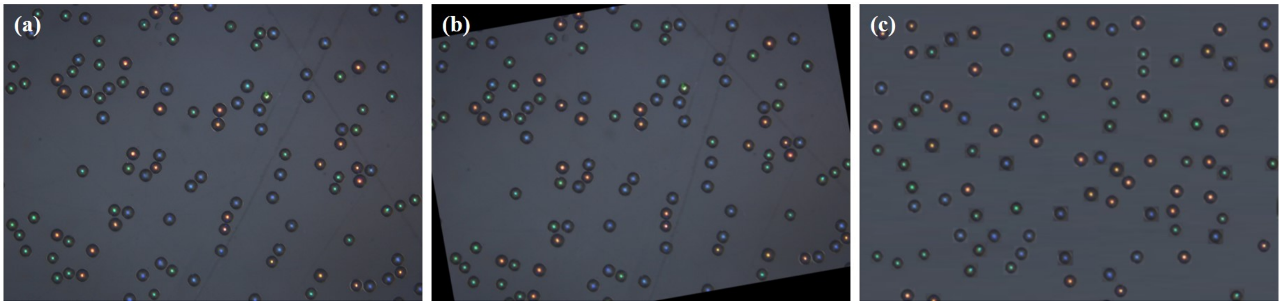


Figure 4: (a) Reference microscope image of a CSR-droplet tag, composed of multicolored blobs. (b) Retake image, *i.e.,* the reference image was resized, rotated, and blurred. (c) Tampered image (generated computationally) composed of random 3-colored blobs.

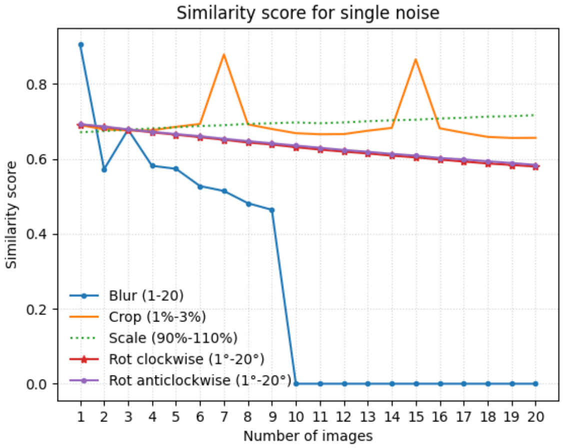


Figure 5: Image Subtraction score for different noise sources.

randomly on a background so to create new images which, despite looking similar, were not generated by reading out from any of our 12 CSR tag. Figure 4-c depicts an example of a fake readout image.

Retakes images for validation. We have further generated one independent set of 2000 mutated and one of 1000 simulated images for further independent validation of our methodology.

4.2 Implementation

Image Subtraction Score and Blob Extraction Score are both meant to measure the level of similarity between t (the image supposed to be a retake of $w_0(x)$) and $t_0(x)$ (the reference readout of $w_0(x)$ stored for authentication). Both implementations rely on a common step: aligning t and $t_0(x)$.

Alignment. We use the Scale-Invariant Feature Transform (SIFT) algorithm (OpenCV[6] library) that enables to detect the features of different transformation operations, *i.e.,* translation, re-scaling, rotation, and illumination changes [13]. We used the Random Sample Consensus (RANSAC) method to *extract key points* representing the features of images and *compute the homography matrix* which represents the transformation for the alignment. The quality of the computed homography relies on the number of inliers. Once the homography matrix is obtained, we calculate the aligned image, $\bar{t}$.

Depending on how 'far' or 'close' the images are the alignment fails or succeeds, respectively. Figure 6 shows an aligned image in case of success (a), and an aligned image in case of failure (b). According to our observation, the alignment fails (thus, the aligned image is not meaningful) when the number of matching key points found (MIN_MATCH_COUNT) is less than 10.

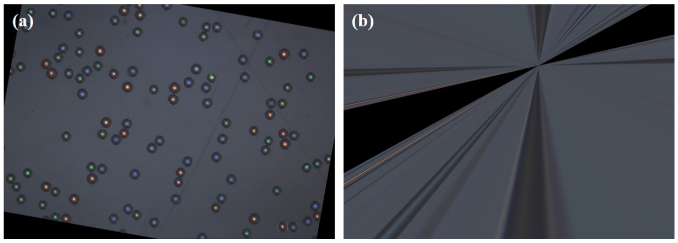


Figure 6: (a) Aligned image between a reference image and a mutated image. (b) The colored (gray) area correspond to the regions where the alignment was attempted.

Image Subtraction Score. If the alignment fails, the score is set to 0. Otherwise, we analyze the difference between $\bar{t}$ and $t_0(x)$ as images. The score, which we indicate with $Score_{sim}$, is calculated as the fraction of *zero-content pixels in the difference matrix*: the score measures the ratio of perfect matching at pixel level:

$$Score_{sim} = \begin{cases} 0, & \text{if } \texttt{MIN\_MATCH\_COUNT} < 10 \\ \frac{|\text{ZeroPixels}[\text{ImageDiff}[\bar{t}, t_0]]|}{|\text{Pixels}[\text{ImageDiff}[\bar{t}, t_0]]|}, & \text{otherwise} \end{cases}$$

Blob Extraction Score. If the alignment fails, the score is set to 0. Otherwise, we first select and then count the number of blobs that match across the $\bar{t}$ and $t_0(x)$. The fundamental tool used in this part is the *blob detection algorithm* from the scikit-image library [24]. First, we convert the *images into gray-scale*, then we compute the *histogram matching.* This transformation adjusts the pixel intensity of the aligned images according to the illumination and contrast of

[6] Open Source Computer Vision Library – opencv.org

the reference image. Once performed this matching distribution, we extract the positions and radii of blobs of the reference image (gray-scale) and the aligned image (after histogram matching) using the blob detection algorithm. We then *extract the colors of the blobs*, using the found blobs as a mask. To calculate the color code, we consider a 4×4 window of pixels and obtain the average of pixel values over the window for each blob, and then find the index of the maximum value for this window. Therefore, the color index is encoded as 0, 1 and 2 for red, green, and blue, respectively. Figure 7 shows this process in images, but the blobs features and colors are also explicitly stored internally as lists of circles and RGB codes, respectively.

We compare the blobs found in the reference image with the blobs found in the second image. If the Euclidean distance between two blobs is smaller than a threshold distance (enough to conclude that the two blobs' centers are geometrically close) and if the color code of the blob regions are the same, we count these blobs as a match. In this way, we implement MatchingBlobs, the set of matching blobs. The implementation can be designed to run in $O(n \log n)$ time, n being the number of blobs. We calculate Blob Extraction Score, here called $Score_{match}$, according to the formula (4).

5 EXPERIMENTS AND EVALUATION

We used an Alienware Aurora R11 desktop with Intel(R) Core(TM) i3-10100 CPU @ 3.60GHz (8 Cores), 32 GB RAM with 64-bits Ubuntu 20.04 LTS Operating System. The computational environment used was PyCharm 2020.3.3 (Professional Edition), Runtime version: 11.0.9.1+11-b1145.77 AMD64. We used Python 3.8.7 as a language of choice, the dataset and source code are available at: https://gitlab.uni.lu/irisc-open-data/2021-nofakes. One of the authors implemented the algorithms, also using Wolfram Language (in Wolfram Language Lab 12.2 on a laptop with Intel Core i7-8550U CPU, running MS windows 10) for validation and control. The results of both implementations are consistent[7].

To evaluate reliability and robustness (section 3), we set the following experiment: we compared each reference image first against its 400 retake images, then against the 800 other retakes, and then against the 1000 simulated images (*i.e.,* the fakes), for a total comparisons as reported in Table 2.

In a non-optimized implementation, calculating $ImageSubtraction$ takes approximately 0.295 ± 0.09 seconds, whereas calculating $Score_{match}$ takes around 20 ± 4.6 seconds. The execution time for calculating $Score_{match}$ has large variance since the complexity of extracting the blobs depends on the structure of the image (*i.e.,* its blob density). However, in a *parallel* implementation, the execution time was reduced to approximately 2.60 seconds using 6 cores.

For each pair in the comparison, we calculated $Score_{sim}$ and $Score_{match}$. From the scores distribution of each reference image compared with its retakes, we estimated the robustness of our algorithm in terms of intra-distance and false negative ratio; from the score distribution of each reference image compared with the set of references and retakes from other images, we estimate the reliability, in terms of inter-distance and false positive ratio; from the score distribution of each reference image compared with the simulated fakes, we estimate the security, in terms of false positive ratio. Here, we intended to play an adversary challenging the authentication procedure.

Table 2: Summary of the dataset.

Operation	Type	Group	Number of comparisons
Blurring Rotation Scale	Intra-distance	Benchmark	4 800
		Validation	2 000
	Inter-distance	Benchmark	21 000
		Validation	12 000

As explained in the previous section, a proper alignment is necessary for both implementations to work. To see why this is necessary, let us consider Figure 6 which shows the results of two alignments. Figure 6-a shows the aligned form of Figure 4-a and Figure 4-b. In contrast, Figure 6-b shows the inability to achieve a proper alignment between the same reference image and the fake image (Figure 4-c). In case of alignment failure, there are none or very few matching blobs, and this should happen only when the pictures are in fact non-correlated *i.e.,* when they are not retakes of the same CSR tag.

5.1 Benchmark Assessments

In addition to false positive and negative ratios, a benchmark for robustness and reliability is to assess that minimum value of the matching score for images that are retakes (with noise) of the same CSR tag (intra-distance) is higher than the maximum matching score obtain by comparing a reference image and the images of retakes of different CSR tags (inter-distance), Equation 5. That is:

$$\min_i \left(D^{intra}_{w_i}(x)\right) > \max_i \left(D^{inter}_{w_i}(x)\right) \tag{5}$$

where

$$D^{intra}_{w_i}(x) = \{\text{Score}[t_i(x), t'_i(x)]|\ \forall t'_i\}$$
$$D^{inter}_{w_i}(x) = \{\text{Score}[t_i(x), t'_k(x)]|\ \forall k \neq i,\ t'_k\}$$

A score that satisfies (5), neatly separates what is recognized as an original from what is rejected as something different. Statistics on intra-distance also are functional to assess the robustness of our score functions.

5.1.1 Results. Figure 8 shows the number of detected blobs as a function of the matching score. It is observed a clear separation between the intra- and inter-distance clusters, fulfilling the condition given in Equation 5.

Figure 9-a shows the number of detected blobs of each reference image after alignment with its respective retake images.

Figure 9-(b-c) depict the result of a classical statistical analysis on the scores. Figure 9-b shows the means and standard deviations (and outliers) for $Score_{sim}$, while Figure 9-c shows them for $Score_{match}$, which is constantly better than $Score_{sim}$.

This suggests the hypothesis that the design based on minutiæ recognition (*i.e.,* Blob Extraction) is more insightful and robust than the design based on image processing (*i.e.,* Image Subtraction). This argument holds even if the absolute values that we obtain for the scores are based on a scoring function which is linear on

[7] The code is available on demand.

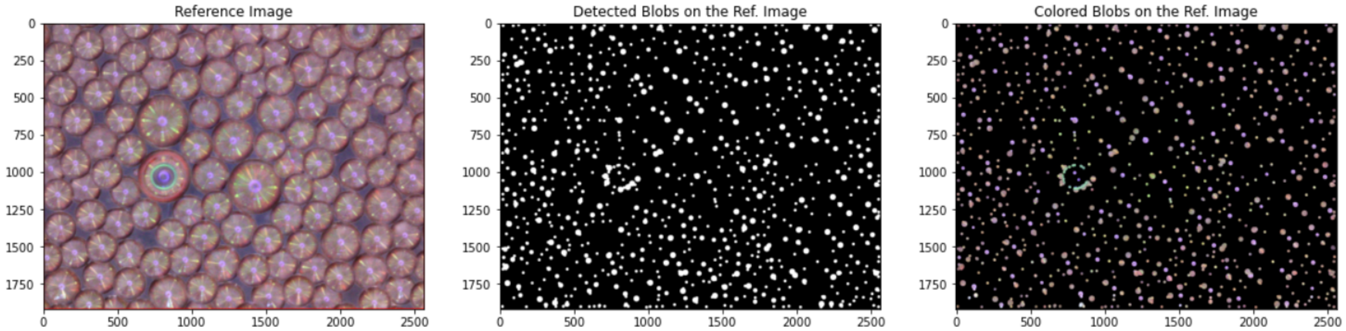

Reference Image
Detected Blobs on the Ref. Image
Colored Blobs on the Ref. Image
0
250
500
750
1000
1250
1500
1750
0
500
1000
1500
2000
2500

Figure 7: (*Left*) Reference CSR image: it is observed the central spot of light in each shell and the photonic cross-communication between the neighbors spheres. (*Middle*) Blobs detection of the reference image. (*Right*) Masked image between the detected blobs and the reference image.

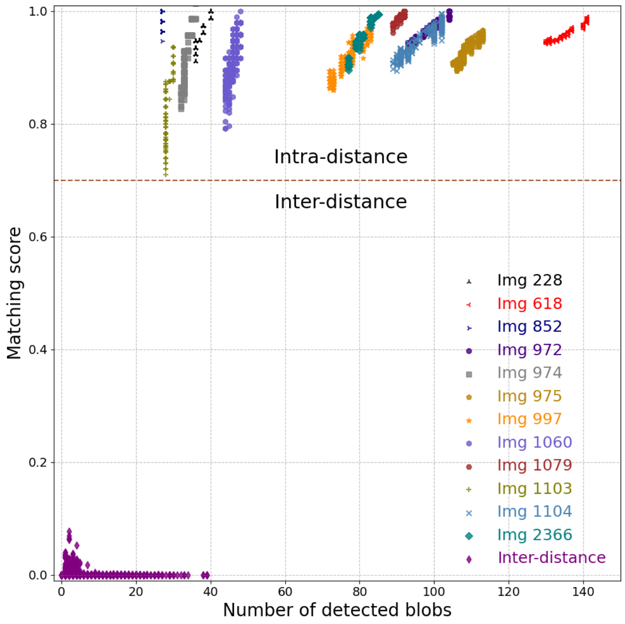


Figure 8: It is observed a clear separation between the intra-distance and the inter-distance values.

the number of matching, mainly mirroring the ratio of matching pixels and of matching blobs, respectively. Using a linear function as a score means that small differences still can cause significant variations in the resulting score values although this do not seem to affect our benchmark negatively, as Figure 8 demonstrates. We are currently looking at using different function scores, for instance, sigmoidal or logit functions commonly used in data science [21], but this research is till ongoing.

In Figure 9-c, we observe that `Img 1103` presents a higher variance. This is justifiable because of the blob size, which are larger in this particular image. Our distance between blobs' centers works for most of the images, but for larger blobs can present a noticeable variance. If we decide that two blobs match when their centers are at, say δ number of pixels one from the other, very large blobs that geometrically intersect can be discarded. We can, in this case, change the implementation that decides when two blobs matches on the basis of the percentage of their overlapping as circles. We tested this variant in our Wolfram Language implementation, proving the concepts that indeed this new blobs matching method removes the outliers in `Img 1103`. Implementing this new algorithm in the Python code and making new experiments with it is a future work.

We also observed that for high blurring values, the scores may also present high variance, since the current blob detection implementation relies on corner detection methods, where pixel discrepancy becomes important. Therefore, whenever the original blobs are not sharp and dense, blurring amplifies the effect, reduces the image quality, and produces misalignment when the window size of the blurring is increased, as shown in Figure 5 (blue line).

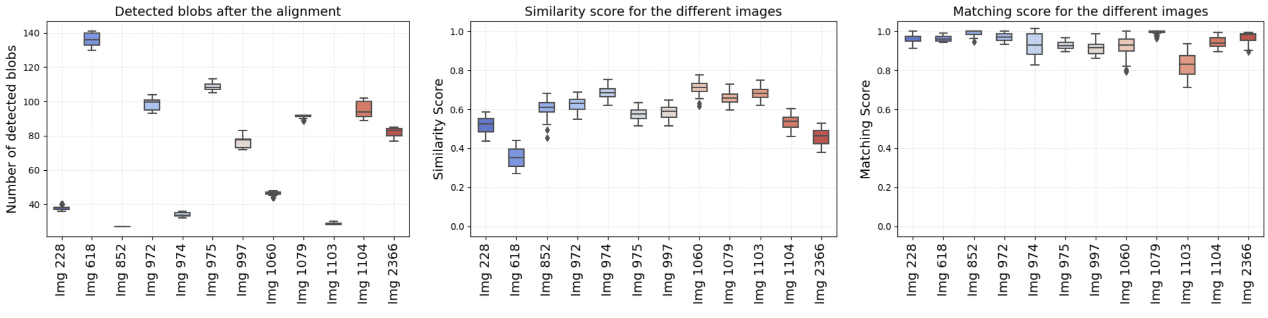
5.1.2 Matching. On the ground of the experimental results, we tuned our implementation for IsMatching on the basis of the results obtained for $Score_{sim}$ ad $Score_{match}$ and upon a threshold (*i.e.,* an acceptance interval). Figure 10 depicts that there is a trade-off between the correct authentication probability and false positives according to the choice of a threshold.

Choosing the threshold value to 5%, the expected authentication probability for correctly identifying a retake image is 1.0 for both similarity score and matching score. In contrast, the corresponding expected probability for incorrectly flagging a simulated image as identical to a reference image is 0.00009 and 0.0002, respectively. For threshold values equal to or higher than 7%, the false-positive ratio drops to 0.0, for both scores. Therefore, assuming a reliable alignment, the choice threshold of 5% is a reasonable choice as the threshold for our authentication decision making. We set the threshold to this value for the validation.

5.2 Validation

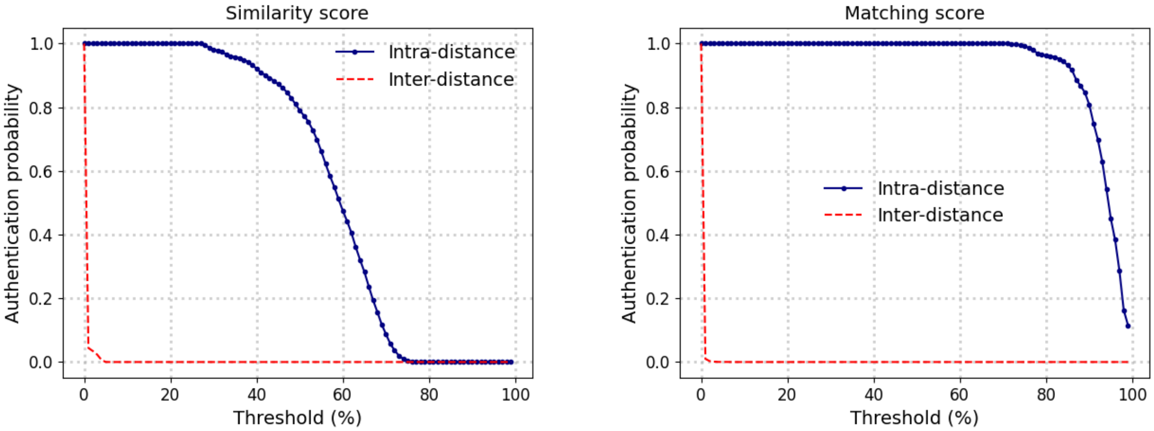
We have further generated an independent set of 2000 mutated and 1000 simulated images for the validation, by randomly choosing the noise to apply within our set of noise ranges.

We calculated $Score_{sim}$ and $Score_{match}$ for the pairwise comparison of the images. We set the threshold value to 5% and counted the number of authenticated tags for this value. Table 3 summarizes



(a) (b) (c)

Figure 9: (a) Number of detected blobs after the alignment. Summary of distribution values for (b) $Score_{sim}$, (c) $Score_{match}$.



(a) (b)

Figure 10: Threshold (%) vs. Authentication probability for (a) $Score_{sim}$, and (b) $Score_{match}$.

the results of this experiment. We observe that the mutated images present the highest authentication scores for all images.

We observe that none of the simulated tags have been incorrectly authenticated (*i.e.,* no false positive) even though for `image 972` we get some non-zero score. The tampered tag used as a fake is inspired by this image (as seen in Figure 1-c); thus, the alignment algorithm attempted to identify some related regions to the reference image, but both scores performed very low (as seen in Figure 8). This suggests that to beat an adversary that knows how the responses of a particular CSR tag look like, we should indeed use the full fledged PUF features of CSRs, for instance by having more runs of challenge-response in the authentication protocol, an improvement that we leave as future work. Nevertheless, if we increase the threshold to 7%, none of the simulated images is authenticated. These results are compatible with the findings discussed in Section 5.1.2.

Table 3: Authentication scores for retakes and simulated images for a threshold equal or lower than 5%.

Image	Retakes		Faked	
	$Score_{sim}$	$Score_{match}$	$Score_{sim}$	$Score_{match}$
228	1.0	1.0	0	0
618	1.0	1.0	0	0
852	1.0	1.0	0	0
972	1.0	1.0	0.016	0.013
974	1.0	1.0	0	0
975	1.0	1.0	0	0
997	1.0	1.0	0	0
1060	1.0	1.0	0	0
1079	1.0	1.0	0	0
1103	1.0	1.0	0	0
1104	1.0	1.0	0	0
2366	1.0	1.0	0	0

5.3 Limitation

We used real CSR tags, but we simulated the possible retakes. As we explained, simulating noisy images is a standard procedure and allows us to control the noise better. We have generated much larger data sets than we could achieve if we had taken retakes by hand. Another limitation is that, in generating the simulated images, we have not simulated an adversary trying hard to subvert our scores, for instance, by using generative adversarial neural networks. This is left for future work. The validation data set is different from the one we have used to tune the threshold, but it is not unrelated: we randomly created the mutated and simulated from the same reference set. Ideally, we should have used a fresh set of CSR tags, but they were not available: producing new tags is not a streamlined process and requires time. We plan to overcome these limitations in future work. There is surely a larger set of metrics that we could have applied to test the security of CSR tags in anti-counterfeiting, for instance, those aiming to assess the space dimension of the extracted features, and their randomness. Before this is possible, we need reliable and robust procedures for features extraction, which is what we achieved so far.

6 CONCLUSIONS AND FUTURE WORK

We have studied how to extract information from tags made of Cholesteric Spherical Reflectors (CSRs) in the prospect to use them as anti-counterfeiting technology. CSR tags have been argued to be optical Physical Unclonable Functions (PUFs), but there is almost no implementation for concrete authentication procedure with the exception of [12], which contains only preliminary results and with a matching algorithm based on histogram analysis. Here, we have discussed two advanced solution designs, whose working principles rely on a CSR tag response's peculiarities. We implemented, tuned, and tested the procedures for accuracy, performance, and false negative rate on a data set of thousands of realistic and simulated responses generated from 12 real CSR tags. One authentication solution works by image matching; the other by extracting and matching colored circles (called blobs) that are recognizable in a CSR tag's optical response.

We used thousands of other mutated and simulated images for our method's validation. Image quality as well as the number and distribution of the droplets are factors that affect the overall authentication performance, but our results confirm that our procedure is able to distinguish authentic from unauthentic retakes of an original tag. Considering other intrinsic properties of CSRs such as cheapness, unclonability, and the ability to shape them in any desired way, this work brings further evidence for a successful use of CSR tags in anti-counterfeiting.

Future work. Our scores are simple linear functions. This means that the score starts growing even when the percentage of matching is small and this is counter intuitive. A matching score that reflects a degree of likelihood should remain very low until the matching reaches an observed mean value and with an increment that depends on the standard deviation experimentally observed. Scores based on *sigmoid* or *logit* functions seem capture better this intuition.

The work for tuning the authentication decision threshold will also require a few iterations, and needs further experiments before being set to a stable value or interval.

Additionally, it will be important to assess the security of the authentication, *e.g.,* testing the authentication quality assuming an adversary that deliberately tries to use the best possible fake physical tags (*e.g.,* holograms) in attempts to fool authentication. Against such an adversary, it will be critical to extend the authentication process with an authentication protocol taking advantage of the capability of CSR tags's acting as a PUF, *i.e.,* that requires successful authentications for *multiple*, randomly chosen, challenge-response combinations, as mentioned above. While each challenge-response combination needs to be implemented, the algorithms and procedures developed here are pivotal elements for authentication. In a real-world implementation, we need to control the read-out for the different challenges: for instance, if one of the challenges is polarization, we need to control this variable when we take a picture. These challenges may require engineering efforts but represent no fundamental roadblocks.

An additional challenge–response combination that is much easier to implement technically than illumination angle variation is to probe the response to different light polarization. This can be done by inserting or removing simple circular polarizers, such as those used in 3D cinema goggles, a task that can easily be automatized in a device with a small physical footprint. While the CSRs used in this study had different colors but identical polarization of the reflected light, it is easy to combine CSRs reflecting with right- and left-handed circular polarization, respectively, in the same tag. Since the difference in polarization is not detectable without polarizers, incorporating polarization as a challenge may be very efficient in distinguishing fake tags that attempt simulating a particular response.

Another future work is to use Deep Neural Networks (DNN). They have been one of the major environments for image processing applications, showing ability to represent images efficiently under various conditions. Recent techniques, such as Residual Networks (ResNet), particularly outperform when applied for image classification [26] although they are only as good as the training input. How they will perform with CSR tag images is an open question, while would be interesting to compare a DNN based matching implementation with the solution presented in this paper.

The last future work, indeed on-going, is to study the use of fuzzy extractors and of secure sketches on our CSR tag's readout images or blob structures. These techniques, the first aiming at extracting nearly uniform binary data from potentially noisy inputs and the second employed to produce public keys from a datum which has to remain secret, have been successfully applied in the processing PUFs for user authentication *e.g.,* see [23]. This is also a key step for the set up of cryptographic protocols based on challenge-response pairs coming from PUF outputs of CSR tags under different illumination conditions which we plan a next step study.

ACKNOWLEDGMENTS

The authors acknowledge the financial support from the Luxembourg National Research Fund (FNR) projects Security in the Shell "SSh" (C17/MS/11688643), and No more Fakes "NoFakes": (PoC20 / 15299666 / NOFAKES-PoC). The authors acknowledge Prof. J. Lagerwall, Dr. Y. Geng, and Dr. H. Agha for their valuable comments and feedback on the manuscript.

REFERENCES

[1] Frederik Armknecht, Roel Maes, Ahmad Reza Sadeghi, François Xavier Standaert, and Christian Wachsmann. 2011. A formal foundation for the security features of physical functions. In *Proceedings - IEEE Symposium on Security and Privacy*. IEEE, Oakland, CA, USA, 397–412. https://doi.org/10.1109/SP.2011.10

[2] Frederik Armknecht, Roel Maes, Ahmad Reza Sadeghi, Berk Sunar, and Pim Tuyls. 2009. Memory leakage-resilient encryption based on physically unclonable

functions. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 5912 LNCS. Springer, Berlin, Heidelberg, Tokyo, Japan, 685–702. https://doi.org/10.1007/978-3-642-10366-7_40

[3] Riikka Arppe and Thomas Just Sørensen. 2017. Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nature Reviews Chemistry* 1 (2017), 1–13. https://doi.org/10.1038/s41570-017-0031

[4] Riikka Arppe-Tabbara, Mohammad Tabbara, and Thomas Just Sørensen. 2019. Versatile and Validated Optical Authentication System Based on Physical Unclonable Functions. *ACS Applied Materials and Interfaces* 11, January (2019), 6475–6482. https://doi.org/10.1021/acsami.8b17403

[5] Hyung Jong Bae, Sangwook Bae, Cheolheon Park, Sangkwon Han, Junhoi Kim, Lily Nari Kim, Kibeom Kim, Suk Heung Song, Wook Park, and Sunghoon Kwon. 2015. Biomimetic microfingerprints for anti-counterfeiting strategies. *Advanced Materials* 27, 12 (2015), 2083–2089. https://doi.org/10.1002/adma.201405483

[6] Qifeng Chen, Xue Li, and Guangxue Chen. 2021. Vegetable oils based UV-luminescent ink for screen printed anti-counterfeiting marking. *Progress in Organic Coatings* 151 (2021), 106009.

[7] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. 2008. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* 38, 1 (jan 2008), 97–139. https://doi.org/10.1137/060651380 arXiv:0602007 [cs]

[8] Yong Geng, JungHyun Noh, Irena Drevensek-Olenik, Romano Rupp, and Jan Lagerwall. 2017. Elucidating the fine details of cholesteric liquid crystal shell reflection patterns. *Liquid Crystals* 44, 12-13 (2017), 1948–1959.

[9] Yong Geng, Junghyun Noh, Irena Drevensek-Olenik, Romano Rupp, Gabriele Lenzini, and Jan P.F. Lagerwall. 2016. High-fidelity spherical cholesteric liquid crystal Bragg reflectors generating unclonable patterns for secure authentication. *Scientific Reports* 6 (may 2016), 1–9. https://doi.org/10.1038/srep26840

[10] Xudong Jiang and Wei-Yun Yau. 2000. Fingerprint minutiae matching based on the local and global structures. In *Proc. of the IEEE 15th Int. Conf. on Pattern Recognition (ICPR-2000), Barcelona, Spain, September 3 - 7, 2000.* IEEE, Barcelona, 1038–1041.

[11] Ji Lee, Hyung Hong, Ki Kim, and Kang Park. 2017. A Survey on Banknote Recognition Methods by Various Sensors. *Sensors* 17, 2 (feb 2017), 34. https://doi.org/10.3390/s17020313

[12] Gabriele Lenzini, Samir Ouchani, Peter Roenne, Peter Y.A. Ryan, Yong Geng, Jan Lagerwall, and Jung Hyun Noh. 2017. Security in the shell: An optical physical unclonable function made of shells of cholesteric liquid crystals. *2017 IEEE Workshop on Information Forensics and Security, WIFS 2017* 2018-Janua (2017), 1–6. https://doi.org/10.1109/WIFS.2017.8267644

[13] David G. Lowe. 2004. Distinctive Image Features from Scale-Invariant Keypoints. *International Journal of Computer Vision* 60, 2 (nov 2004), 91–110. https://doi.org/10.1023/B:VISI.0000029664.99615.94

[14] Roel Maes. 2013. *Physically Unclonable Functions: Constructions, Properties and Applications.* Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-41395-7

[15] Kalyani Mali and Samayita Bhattacharya. 2001. Fingerprint Recognition Using Global and Local Structure. *Int. J. of Ad. Trends in Computer Science and Engineering* 15 (2001), 1952 – 1964.

[16] Thomas McGrath, Ibrahim E. Bagci, Zhiming M. Wang, Utz Roedig, and Robert J. Young. 2019. A PUF taxonomy. *Applied Physics Reviews* 6, 1 (2019), 011303–(1–25). https://doi.org/10.1063/1.5079407

[17] Junghyun Noh, Hsin Ling Liang, Irena Drevensek-Olenik, and Jan P.F. Lagerwall. 2014. Tuneable multicoloured patterns from photonic cross-communication between cholesteric liquid crystal droplets. *Journal of Materials Chemistry C* 2, 5 (feb 2014), 806–810. https://doi.org/10.1039/c3tc32055c

[18] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. 2002. Physical One-Way Functions. *Science* 297, September (2002), 2026–2031. https://doi.org/10.1126/science.1074376

[19] Mathew Schwartz, Yong Geng, Hakam Agha, Rijeesh Kizhakidathazhath, Danqing Liu, Gabriele Lenzini, and Jan P F Lagerwall. 2021. Linking physical objects to their digital twins via fiducial markers designed for invisibility to humans. *Multifunctional Materials* 4, 2 (jun 2021), 1–19. https://doi.org/10.1088/2399-7532/ac0060

[20] Mathew Schwartz, Gabriele Lenzini, Yong Geng, Peter B. Rønne, Peter Y.A. Ryan, and Jan P.F. Lagerwall. 2018. Cholesteric Liquid Crystal Shells as Enabling Material for Information-Rich Design and Architecture. *Advanced Materials* 30, 30 (2018), 1–19. https://doi.org/10.1002/adma.201707382

[21] Steven S. Skiena. 2017. *The Data Science Design: Manual.* Springer, Stony Brook, NY - USA.

[22] Bin Song, Houyu Wang, Yiling Zhong, Binbin Chu, Yuanyuan Su, and Yao He. 2018. Fluorescent and magnetic anti-counterfeiting realized by biocompatible multifunctional silicon nanoshuttle-based security ink. *Nanoscale* 10, 4 (2018), 1617–1621.

[23] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli. 2017. User Authentication via PRNU-Based Physical Unclonable Functions. *IEEE Transactions on Information Forensics and Security* 12, 8 (2017), 1941–1956. https://doi.org/10.1109/TIFS.2017.2697402

[24] Stefan Van der Walt, Johannes L Schönberger, Juan Nunez-Iglesias, François Boulogne, Joshua D Warner, Neil Yager, Emmanuelle Gouillart, and Tony Yu. 2014. scikit-image: image processing in Python. *PeerJ* 2 (2014), e453.

[25] Shen Wang, Ehsan Toreini, and Feng Hao. 2021. Anti-Counterfeiting for Polymer Banknotes Based on Polymer Substrate Fingerprinting. *IEEE Transactions on Information Forensics and Security* 16 (2021), 2823–2835. https://doi.org/10.1109/TIFS.2021.3067440

[26] Zifeng Wu, Chunhua Shen, and Anton Van Den Hengel. 2019. Wider or deeper: Revisiting the resnet model for visual recognition. *Pattern Recognition* 90 (2019), 119–133.

[27] Yong Xu, David Zhang, and Jing-Yu Yang. 2010. A feature extraction method for use with bimodal biometrics. *Pattern Recognition* 43, 3 (2010), 1106–1115. https://doi.org/10.1016/j.patcog.2009.09.013

[28] Yijing Xun, Zhijiang Li, Xiaolu Zhong, Sheng Li, Jiawang Su, and Ke Zhang. 2019. Dual Anti-counterfeiting of QR Code Based on Information Encryption and Digital Watermarking. In *Lecture Notes in Electrical Engineering*, Vol. 543. Springer Verlag, Shandong, China, 187–196. https://doi.org/10.1007/978-981-13-3663-8_27

[29] Minli You, Junjie Zhong, Yuan Hong, Zhenfeng Duan, Min Lin, and Feng Xu. 2015. Inkjet printing of upconversion nanoparticles for anti-counterfeit applications. *Nanoscale* 7, 10 (2015), 4423–4431.