

# Fast and Robust Speckle Pattern Authentication by Scale Invariant Feature Transform algorithm in Physical Unclonable Functions

Giuseppe Emanuele Lio,\* Mauro Daniel Luigi Bruno,† Francesco Riboli,‡ Sara Nocentini,§ and Antonio Ferraro¶  
(Dated: May 1, 2025)

Nowadays, due to the growing phenomenon of forgery in many fields, the interest in developing new anti-counterfeiting device and cryptography keys, based on the Physical Unclonable Functions (PUFs) paradigm, is widely increased. PUFs are physical hardware with an intrinsic, irreproducible disorder that allows for on-demand cryptographic key extraction. Among them, optical PUF are characterized by a large number of degrees of freedom resulting in higher security and higher sensitivity to environmental conditions. While these promising features led to the growth of advanced fabrication strategies and materials for new PUF devices, their combination with robust recognition algorithm remains largely unexplored. In this work, we present a metric-independent authentication approach that leverages the Scale Invariant Feature Transform (SIFT) algorithm to extract unique and invariant features from the speckle patterns generated by optical Physical Unclonable Functions (PUFs). The application of SIFT to the challenge response pairs (CRPs) protocol allows us to correctly authenticate a client while denying any other fraudulent access. In this way, the authentication process is highly reliable even in presence of response rotation, zooming, and cropping that may occur in consecutive PUF interrogations and to which other postprocessing algorithm are highly sensitive. This characteristics together with the speed of the method (tens of microseconds for each operation) broaden the applicability and reliability of PUF to practical high-security authentication or merchandise anti-counterfeiting.

## I. INTRODUCTION

Coherent light that impinges and diffuses into a scattering medium, interferes in the far field producing a granular image referred to as speckle pattern [1, 2]. The speckle is both a challenge and an opportunity in many fields, as it can degrade image quality or provide useful information for measuring surface roughness, displacement, and biological parameters finding therefore applications in various scientific fields spanning from astronomy, imaging, cultural heritage, metrology and crypto-security [3–11]. In the latter, speckle patterns originated by illuminating a rough or light-scattering surface can act as a unique “fingerprint” that is nearly impossible to replicate generating the so called optical physical unclonable functions (PUFs). Due to the possible multiple interrogations and large number of degrees of freedom, PUFs work as on-the-fly generators of secure cryptographic keys [9, 12–15]. Due to their inherent manufacturing errors and internal randomness, it has been demonstrated that reproduction of the same optical PUF is impossible even by the manufacturer itself [16, 17]. Optical strong PUFs are typically used within a Challenge Response Pairs (CRPs) protocol that includes an enrollment and verification process. In both steps, the scattering sample is illuminated with multiple pseudo-random challenges ( $C$ ) and the corresponding responses ( $R$ ) are collected by a camera. During the enrollment process, a large database of CRPs is stored at the central authority as reference and the PUF is then delivered to the client.

The prover authentication is then based on the analysis of speckle pattern images that, at first, are post-processed and then analyzed by statistical methods where parameters such as contrast, correlation length, and intensity distribution are used to quantify speckle characteristics [9, 18, 19]. Post-processing can be performed using standard image transformation (e.g. the Gabor hashing or wavelet decomposition) and binarization algorithms. Along this process, the wavelength of a wavelet-based Gabor filter is tuned to extract the relevant features of the speckle images, both ensuring the repeatability of the responses under the same challenge interrogation and preserving the random nature of responses to different challenges. The response  $R_i$  (speckles) related to the challenges  $C_i$  is then hashed and reshaped into a 1D binary array or keys  $K_i$ . The pairwise distance between each binary keys  $K_1, \dots, K_i$  is then measured with the Hamming distance metric, i.e. the number of bits that differ in two bit strings[20]. Distances between keys generated by different challenges are called “unlike” distances (and are related to the entropy of the key), while those generated by same challenges are called “like” distances (and are related to the stability of the PUF). Commonly, the

---

\* Istituto di Nanoscienze CNR-NANO, Consiglio Nazionale delle Ricerche, Pisa, 56127, Italy

† Istituto di Nanotecnologia CNR-NANOTEC, Consiglio Nazionale delle Ricerche, Rende, 87036, Italy

‡ CNR-INO - National Institute of Optics, Sesto Fiorentino, 50019, (FI), Italy; Also at European Laboratory for Non-Linear Spectroscopy (LENS), University of Florence, Sesto Fiorentino, 50019, (FI), Italy

§ Istituto Nazionale di Ricerca Metrologica (INRIM), (TO), 10135, Italy; Also at European Laboratory for Non-Linear Spectroscopy (LENS), University of Florence, Sesto Fiorentino, 50019, (FI), Italy; s.nocentini@inrim.it

¶ Istituto di Nanotecnologia CNR-NANOTEC, Consiglio Nazionale delle Ricerche, Rende, 87036, Italy; antonio.ferraro@cnr.it

Fractional Hamming Distance (FHD) metric, the Hamming distance normalized by the bit string length, is also used to compare the binary keys that are retrieved from the speckle patterns recorded during the authentication with the ones of the database collected during the enrollment. Moreover, the currently employed analysis approaches suffer from a high sensitivity to minimal variations of the speckle pattern that may occur in case of minimal variation of the position, illumination and rotations that may lead to a failure in the PUF authentication[17].

In this scenario, it is of paramount importance to find a new, flexible analysis method for fast processing of speckle pattern. Image recognition algorithms enables the analysis of images to extract relevant information and features. These algorithms are being improved at fast pace and are now used in daily life in many sector such us logistic, security access, healthcare, traffic management and so on [21]. Scale-Invariant Feature Transform (SIFT) [22, 23] represents a valid and versatile method for detecting and extracting distinctive local features from an image [24, 25]. A key characteristic is the ability to recognize unique features of the image under analysis also under transformations such as scaling, rotation and illumination variations. This robustness has made SIFT widely utilized in computer vision tasks, particularly in object recognition and image matching [26]. A decade ago, a preliminary work using SIFT for speckle recognition shown how it improves the accuracy identification with respect to correlation analysis in tens of seconds [27]. Based on this study, more recently, we leverage on its capability of extracting unique and stable features for anti-counterfeiting applications. Specifically, SIFT enables the identification and authentication of security tags by detecting keypoints, comparable to a fingerprint. These features serve as digital signatures, which can be stored and subsequently compared against a reference database for verification purposes [28–30]. It is remarkable that for human fingerprints, a minimum number of 20 unique features matches is enough to agree with the identity of the designed subject [31].

In this work, we present a straightforward approach based on Scale-Invariant Feature Transform (SIFT) algorithm for rapid and robust identification and validation of strong optical PUFs whose speckle patterns generated through the Challenge-Response Pair (CRP) protocol. To demonstrate the effectiveness of our approach, we fabricated three distinct types of optical PUFs, each characterized by different scattering properties. The first type is fabricated by dispersing polystyrene (PS) nanoparticles (NPs) onto a glass substrate. The second involved the realization of a polymer-dispersed liquid crystal (PDLC) structure, while the third is based on titanium dioxide ( $TiO_2$ ) nanoparticles embedded within a polymer matrix. We refer to these implementations as PS-PUF, PDLC-PUF, and  $TiO_2$ -PUF, respectively. The produced speckle patterns were acquired, stored into different datasets and processed on-demand through the SIFT algorithm. To prove the reliability of the proposed method, speckle patterns underwent distortion such as rotation, scaling and cropping without affection the identification capability of the SIFT. The ability of SIFT to extract distinctive and stable features from complex speckle patterns underscores its suitability for fast and accurate authentication, paving the way for enhanced security applications in anti-counterfeiting and identification systems.

## II. MATERIALS AND METHOD

### A. Three PUF-Samples and Their Fabrication

We have fabricated and experimentally characterized three PUF-samples. They are made from distinct materials and possess different optical characteristics, such as internal entropy, scatterer size and density, and so-called optical thickness ( $OT$ ), that is the natural logarithm ( $\ln$ ) of the sample transmission. As a simple quantitative example, an optical thickness of 1 indicates that the transmitted/diffused intensity is reduced by a factor of  $1/e$  with respect to the initially incident intensity. Samples with small optical thickness around  $OT \leq 1$ , are almost transparent to a human observer, and the photons traveling through the sample on average undergo only a few scattering events. On the contrary, samples with larger optical thickness  $OT > 1$  make the light bounce multiple times internally among their scattering centers and appear increasingly opaque to the human eye.

The PS-PUF-sample shown in Figs.1a-d consists of a single layer of polystyrene nanospheres of diameters  $d \simeq 250\text{nm}$ , which were randomly deposited on a glass substrate ( $25 \times 25\text{mm}^2$  in x-y-dimensions) by a spin coating process. By tuning the spin coating rotation speed and keeping the other parameters fixed, either a single- or double-layer packing can be obtained. For our purposes, a single layer PUF with thickness around  $250\text{nm}$  in z-dimension was created by using a rotation speed of 2000 rpm. As desired, the sample presents small crystalline regions with a hexagonal close-packed symmetry, few voids, and no double layers. The low refractive index of polymer nanospheres ( $n \simeq 1.59$ ) as well as the single layer geometry leads to a weakly scattering medium and the resulting refractive index contrast is 0.59. Furthermore, it is fully transparent to the human observer, with an optical thickness of  $OT = 0.39$ .

The PDLC-PUF-sample illustrated in Fig1b-e consists of a polymer-dispersed liquid crystal (PDLC) structure, with x-y-dimensions of again  $25 \times 25\text{mm}^2$  and a thickness in z-direction of  $140\mu\text{m}$ . The sample is obtained by an emulsion of liquid crystal molecules (5CB) into a matrix of polydimethylsiloxane (PDMS). The liquid crystals form light scattering droplets with a diameter of around  $10\mu\text{m}$ . Please note that in opposition to our first PS-PUF-sample, we

are no longer forming a single layer in z-dimension, whose thickness is roughly equal to the diameter of its scattering elements. Instead, the thickness of the second PUF-sample is about 15 times the size of its scatterers. The small refractive index contrast between the scatters (droplets made by radially aligned liquid crystal molecules with average refractive index  $n_{av} \simeq 1.6$  at  $25^\circ C$  and wavelength  $\lambda \simeq 633nm$ ) and the polymeric matrix ( $n \simeq 1.43$ ) results in a weakly scattering medium, refractive index contrast of 0.17 and optical thickness less than 1 ( $OT = 0.7$ ). It exhibits a slightly reduced transparency to the human eye.

Finally, the  $TiO_2$  PUF-sample shown in Fig 1c-f consists of Titanium dioxide ( $TiO_2$ ) nanoparticles in a polymeric stabilizing matrix, more precisely in a photopolymer resin. It is made of a commercial UV-curing acrylate optical adhesive with a dispersion of rutile  $TiO_2$  nanoparticles with a diameter of  $280nm$ . The mixture of polymer and nanoparticles is rendered homogeneous through magnetic stirring and an ultrasonic bath for around 1 hour. It is then cured with an UV lamp, resulting in a  $230\mu m$  thick film on a glass substrate. The large refractive index of  $TiO_2$  ( $n \simeq 2.87$ ) compared to the surrounding polymeric matrix ( $n \simeq 1.52$ ) leads to a strong scattering with a refractive index contrast of 1.35. It creates an optical thickness of  $OT = 2.25$ , and a structure that is opaque to human observers. Table I summarizes the properties of the three PUF-samples.

PUF	Scatterer size	Number of Scatterers	Scatterer Density	Optical Thickness	R.I. Contrast
PS	$d \sim 250 nm$	$10^2$	$10^9/cm^2$	0.39	0.59
PDLC	$d \sim 10 \mu m$	$10^6$	$7*10^7/cm^3$	0.7	0.17
$TiO_2$	$d \sim 250 nm$	$5*10^{10}$	$2*10^{12}/cm^3$	2.25	1.35

TABLE I. Properties of the three optical PUFS

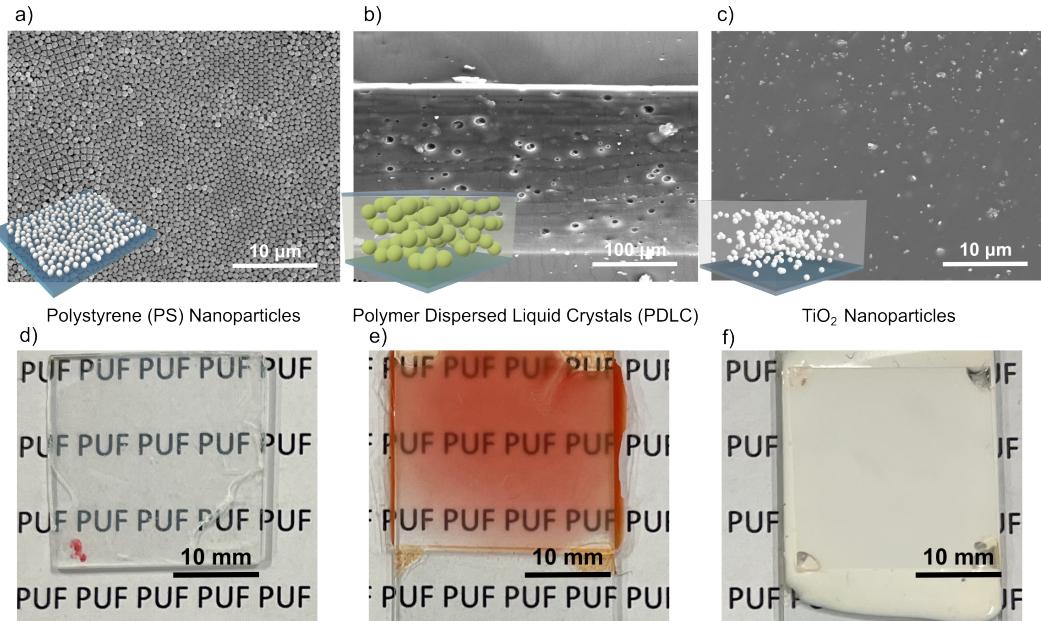


FIG. 1. SEM images and schematic representation of a) PS-PUF constituted by a single layer of polystyrene nanoparticles, b) PDLC-PUF constituted Polymer Dispersed Liquid Crystals PDLC-PUF and c)  $TiO_2$ -PUF constituted by  $TiO_2$  nanoparticles dispersed in a dense polymer matrix. d-f) photographs of the proposed three PUFS.

## B. Challenge Response Pair Protocol and optical apparatus

The optical PUFs were investigated using Challenge Response Pairs (CRPs) protocol [9, 14, 17, 32]. A He-Ne red laser beam with wavelength  $\lambda = 633 nm$  (power 5 mW) propagates through a series of lenses, polarizers, and irises. The beam, after a beam-expander, impinges on a digital micro-mirror device (DMD) used for the spatial intensity modulation of the laser beam that is then conveying the challenge ( $C_i$ ) to the PUF. Each individual  $C_i$  is then projected on the PUF surface and light diffuses through the disordered media. The transmitted light interferes in the far field producing an optical pattern named speckle pattern. This constitutes the PUF response  $R_i$ , which is

collected in cross-polarization configuration to remove any non-scattered light. This pattern is collected by a CCD camera, Thorlabs camera CS165MU. Here, we used a  $270 \times 360$  px camera with 40 FPS for this task. **Figure 2** reports a schematic representation and photos of the experimental setup.

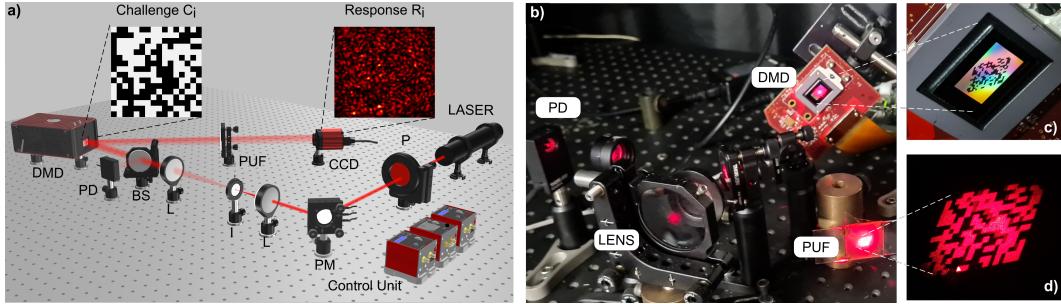


FIG. 2. a) Schematic representation of the experimental setup used to collect the CRPs. b) Real picture of the main part of the setup used to generate and project the challenges. c) The challenge on the DMD, d) the projected challenge on the PUFs.

### C. Scale Invariant Feature Transform analysis

The produced speckle patterns were analyzed using SIFT algorithm, which identifies image features by transforming an image into a vast collection of local feature vectors. These latter, identified as SIFT keys, are invariant to translation, scaling, rotation, and partially to illumination changes in the image [23], making them more robust also in case of fluctuation of the intensity of the laser beam. Four main calculation steps are required to generate all the image features: (a) scale-space extrema detection, done using a Gaussian difference function to identify potential points of interest that are invariant to scale and orientation; (b) key point localization, where key points are selected based on measurements of their stability; (c) orientation assignment, where one or more orientations are assigned to each key point location based on the gradient directions of the local image; and (d) key point descriptor, which describes key points by measuring the local gradients in the image at the selected scale [22]. To analyze and compare the images, a script was used implementing the SIFT algorithm, from OpenCV library, in Python [30]. The SIFT algorithm identifies keypoints and evaluates the typical pixel size using scale-space extrema detection, which relies on differences of Euclidean distances (L2 norm) to detect significant image structures across multiple scales. Then, several parameters are used to configure the feature recognition process, such as the maximum number of features the user wishes to detect, the number of octaves in each Difference-of-Gaussian (DoG) function (with 4 being a commonly recommended value according to OpenCV documentation), and the contrast and edge thresholds, which help in accurately identifying bright and dark features within the image. To construct the first octave, a Gaussian filter is applied to the input image using multiple values of  $\sigma$ . For the second and subsequent octaves, the image is first downsampled by a factor of 1.6, and then Gaussian filters with different  $\sigma$  values are applied. Specifically, Octave 1 uses a scale of  $\sigma$ , Octave 2 uses  $2\sigma$ , and so on. After setting these parameters, a matching distance ( $M_d$ ) is defined. This value quantifies the number of common features detected between two compared images. [33–35]. According to the quality of the collected figures and after optimization procedure, we identified and used for all the analyses the following parameters: the number of recognized features set equal to 0 (it means to find all possible matches) the number of octave layers equal to 4, the contrast and edge threshold equal to 0.04 and 5, respectively. Finally  $\sigma$  has been set at 1.6 and  $M_d$  at 0.7. While these parameters can be finely adjusted based on feature size and image contrast to optimize the number of detected keypoints, we demonstrate that, even with a fixed optical setup, varying the system's optical properties allows the SIFT algorithm to reliably authenticate different primitives.

## III. RESULTS

In order to evaluate the SIFT-based authentication on different types of optical PUFs, we fabricated three primitives that produce transmission speckle patterns with different brightness and contrast. We selected i) a single layer of Polystyrene (PS) NPs on glass, ii) a 3D low refractive index PUF made by a polymer dispersed liquid crystals (PDLC) and iii) a 3D high refractive index medium by dispersing Titanium Dioxide ( $TiO_2$ ) NPs into polymer matrix (for further details see Materials and Method section).

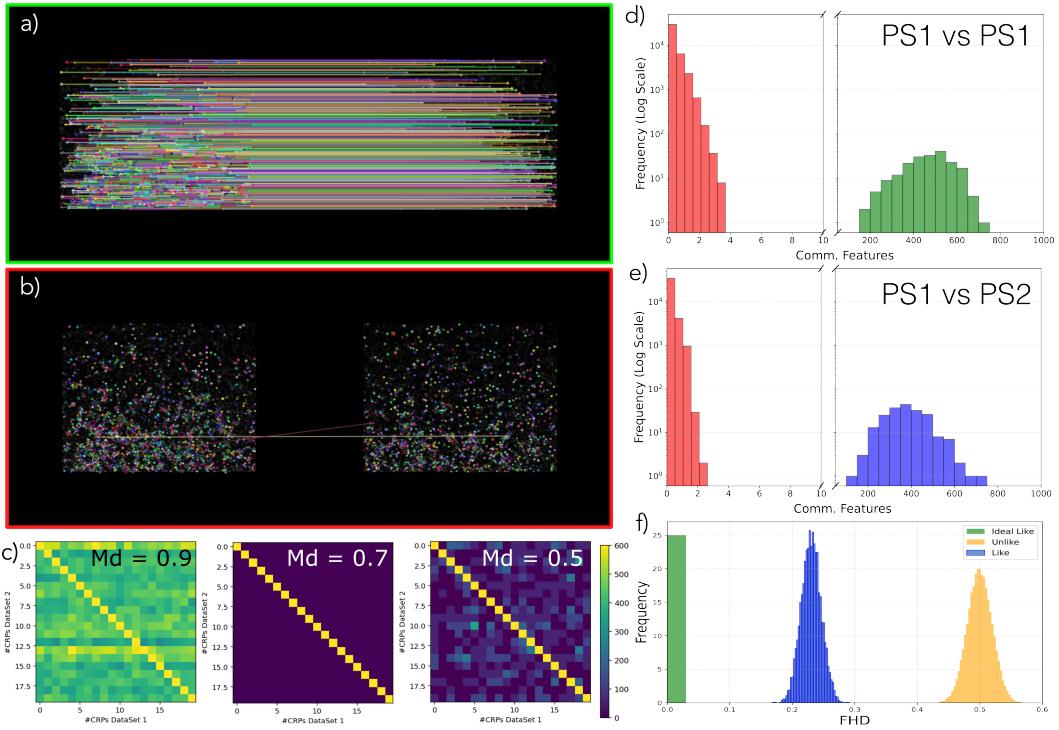


FIG. 3. a–b) Example images showing fully recognized speckles (produced under the same challenge conditions) and cases with no or few recognized points (from different speckles). c) Maps showing recognized points for a comparison of 20 versus 20 speckles, with varying matching distance ( $M_d$ ) parameter value. The scale is the same for the three matrices with a maximum number of recognized point of 600. d) Comparison between 200 versus 200 speckles from the same dataset (PS1). In the histogram the speckles that found their match are reported in green while the other one with no match are reported in red. e) Comparison between 200 versus 200 speckles from two datasets collected at different times (PS1 and PS2). In the histogram the speckles that found their match are reported in blue while the other one with no match are reported in red. f) Fractional Hamming Distance (FHD) distribution calculated over the larger database, illustrating the ‘ideal-like,’ ‘like,’ and ‘unlike’ distributions.

We first investigated the properties of PS-PUF by interrogating it with 200 challenges  $C_i$  and collecting the resulting response  $R_i$  as speckle patterns (see Method section for details). They were then analyzed with the SIFT algorithm and the results reported in **Figure 3**. We refer to this speckle patterns database as dataset PS1 acquired at time  $t_0$ . This analysis results in a database of 40000 comparisons. When comparing each speckle pattern with itself, the algorithm recognizes a large number (a few hundreds) of unique feature matches which are visually indicated as colored linked lines as shown in **Figure 3a**. When the SIFT algorithm is applied to two different responses, the common matched features are few (less than five), namely are false positive, as shown in **Figure 3b**. **Figure 3c** presents three correlation maps of the number of identified features for 20 different speckle patterns varying the matching distance ( $M_d$ ). Herein, the diagonal represents the self-comparison of each speckle pattern with values exceeding 600. The maps show that, for a  $M_d$  value of 0.9 or 0.5, the number of false-positive recognition increases, while a value of  $M_d$  of 0.7 allows to correctly recognize the speckles with themselves indicating this parameter as the best choice for the selected patterns. **Figure 3d** reports the histogram of the number of false positive (red bars) and true positive (green bars) matches for the entire comparison of PS1 database where the green bars correspond to speckles that found a number of matches that overcomes 400 points. The variability of the matched features in between identical speckle patterns depends on the number of speckle grains present in the pattern as well as their contrast. The bars indicate also the number of common features and related occurrence frequency. The red bar, instead, reports the number of comparisons with a few matches found, values that remains below ten points for all the considered speckles. Next, the same PS-PUF was analyzed at a different time using the same CRPs protocol, with the same challenges set ( $C_{i \dots N}$ ). The resulting speckle patterns were acquired to form a new dataset, referred to as PS2 acquired at time  $t_1$ . Both datasets were then used as a database for the SIFT comparison. As shown in Figure 3e, the number of matched points is maximized only for 200 speckle patterns (blue bars), corresponding to the responses ( $R_i(t_0)$  and  $R_i(t_1)$ ) generated using the same challenge ( $C_i$ ). Even if there is a reduction of the common matched features due to environmental fluctuations, it is still possible to clearly recognize each single speckle pattern that have more than 200 common

features. The blue histogram, therefore, is now indicating the stability of the system: the larger number of recognized points the higher is the system stability. In contrast, as expected, all other cross-comparisons ( $R_i(t_0)$  and  $R_j(t_1)$ ) generated from the challenge ( $C_i$  and  $C_j$ ) resulted in only a few recognized matched points (red bar). This confirms the uniqueness and large difference of the responses related to different challenges. As counterproof, we analyzed the speckles pattern datasets (PS1 versus PS2) with the FHD metric, see **Figure 3f**. By comparing the speckle  $R_i(t_0)$  from PS1 with  $R_j(t_1)$  from PS2, which are the outputs produced by the same  $C_i$ , we obtain a "like" distribution (indicated in blue) with a mean value at 0.23. Hence, the blue histogram shown in Figure 3e can be considered the analog of the "like" distribution reported in the FHD analysis. The recognized responses represented in the blue histogram exhibit a shift in the number of common features toward lower values similar to the FHD "like" distribution, that shifts towards larger FHDs with respect to the ideal value (green bar). On the other hand, when comparing speckle responses generated using different input challenges ( $C_i$ ), an "unlike" distribution is obtained, peaked at around 0.5, as expected. This analysis confirms that the speckle patterns produced by different challenges are inherently distinct, thereby demonstrating the capability of the proposed PUF to generate unique, but reproducible responses with no false-positive matches in the SIFT analysis. As with the FHD metric, the clear separation between the "like" and "unlike" distributions in the SIFT approach enables the definition of an authentication threshold that minimizes the false positive. For the PS-PUF, a threshold of approximately 100 common features can be adopted to ensure reliable authentication. Given this characterization, we evaluated the effectiveness of the proposed SIFT-based approach in

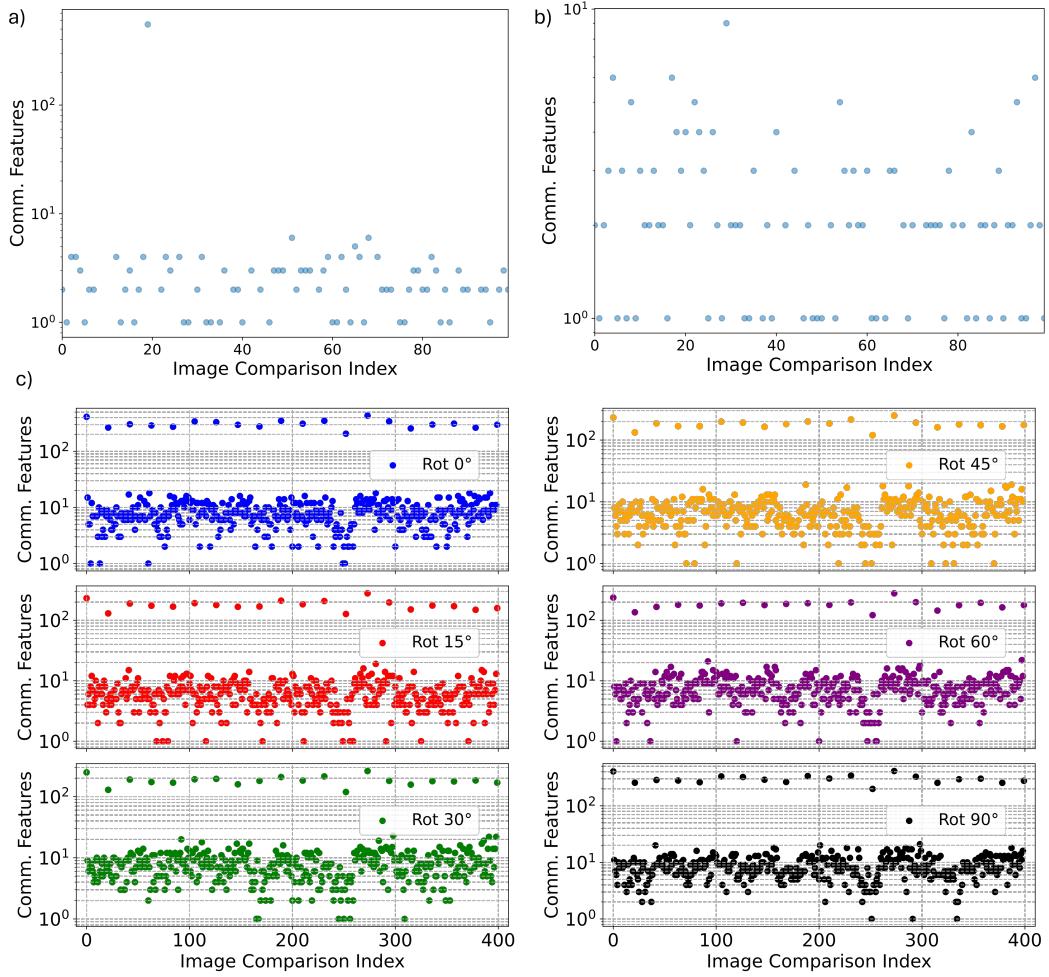


FIG. 4. Comparison, using SIFT analysis, of 1 speckle into a database of 100 speckles which is a) inside, b) outside the database. c) Comparison of speckle patterns, using SIFT analysis, by rotating them at 0°, 15°, 30°, 45°, 60° and 90°

identifying, and hence authenticating, a single speckle pattern referred to as  $S_x$ , within a database, in other words the ability to identify if a speckle is part or not of a certain database (PS1 or PS2). In the cloud of points map shown in **Figure 4a**, where the X-axis indicates the speckle index and the Y-axis the number of common unique features, there is a clear evidence of a single response for which the number of recognized points overcome the authentication threshold

(response #20 having more than 500 common features). In contrast, all other speckles exhibit only a few common features, which can be considered as “false positives.” To further validate this approach, we repeated the analysis considering a target speckle  $S_y$ , e.g. the response produced by challenge 150, that is outside the database. The results, presented in **Figure 4b**, show that for all speckle patterns (again 100) in the database, only a few “false positive” matches were detected. Please note that on Y-axis the maximum value now is 10. This confirms that when the queried speckle is absent from the database (PS1 or PS2), SIFT does not falsely identify any pattern. These findings demonstrate that once a dataset is established, the proposed SIFT-based method can reliably recognize and verify the presence of a unique speckle pattern. One of the strengths of the SIFT method is its invariance to image rotation, a crucial factor when analyzing speckle patterns that are inherently sensitive to even small variations in orientation. In order to confirm such robustness, we analyzed a database of 20 speckle patterns (from PS1) and compared them with themselves after the application of an image rotation (PS1-R) at seven different angles namely  $0^\circ$ ,  $15^\circ$ ,  $30^\circ$ ,  $45^\circ$ ,  $60^\circ$  and  $90^\circ$ . The results, shown in Figure **Figure 4c**, are presented using waterfall plots to illustrate that only for 20 comparisons of the response with itself after rotation, the commonly matched features overcome 100. In contrast, for all the other possible comparisons, the number of unrecognized features falls in the range in between 1 and 20. This confirms that SIFT effectively preserves its matching accuracy even when speckle patterns undergo significant angular transformations. In the following analysis, we performed an additional test to corroborate the robustness of

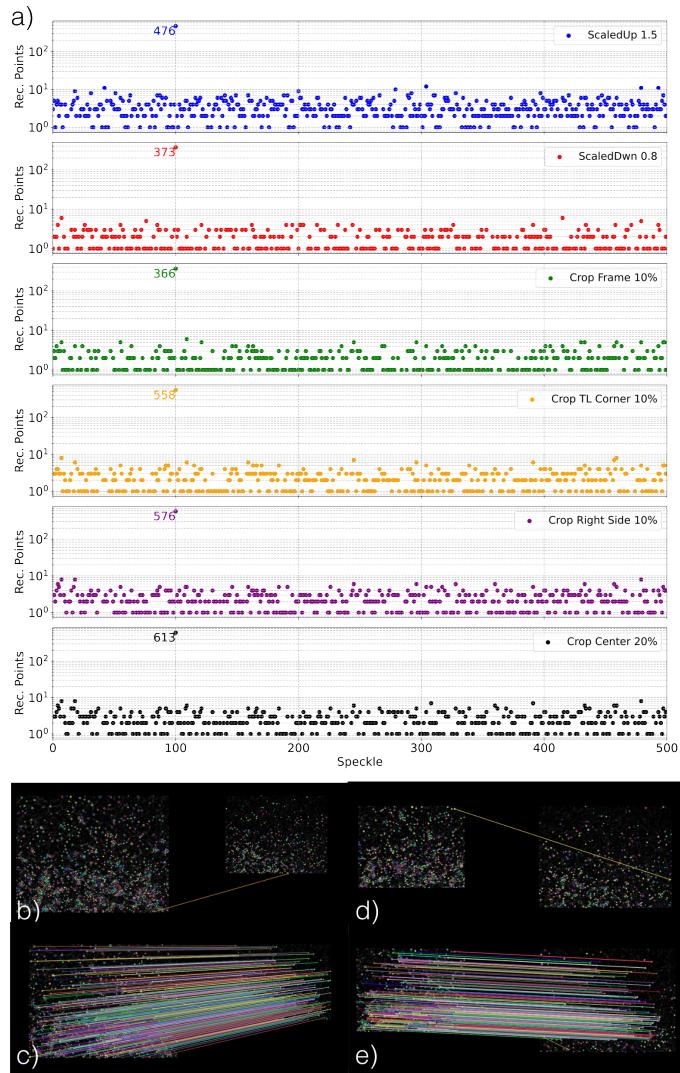


FIG. 5. a) Comparison, using SIFT analysis, of 1 speckle (tag number #100) into a database of 500 ones when scaled-up by 1.5, scaled-down by 0.8, cropped of 10% along the frame, cropped of 10% from the Top-Left (TL) corner, or from the right side and finally cropped of 20% in the center. Zero and full recognized points from scale-up tag (b,c) and cropping the surrounding frame by 10% (d-e).

the SIFT method applied for the recognition of speckle patterns. In fact, SIFT enables fast and reliable identification of a speckle, even when the pattern is subjected to transformations such as scaling or cropping (from all edges or a single side) that can occur for example when using different optical setups. This capability is demonstrated in **Figure 5a**, where SIFT successfully detects and verifies the presence of the speckle under consideration despite these modifications. The SIFT protocol was tested by checking the correct identification of the speckle pattern #100 after different image transformations within a database of 500 speckle patterns. The speckle pattern #100 was subjected to: scaling-up by 1.5, scaling-down by 0.8, cropping of 10% along the frame, cropping of 10% from the Top-Left (TL) corner, or from the right side and finally cropping of 20% in the center. The results, illustrated in **Figure 5a**, confirm that even when the target speckle pattern (#100 for this case) undergoes such transformations, there are a large number of matched features, well above the authentication threshold only in the correspondence of speckle #100 inside the database, demonstrating therefore high specificity and accuracy. **Figure 5b–e** shows clear cases of successful and failed recognition. Specifically, it reports zero and full feature matches in two test scenarios: one where the speckle pattern was scaled up by a factor of 1.5 (b,c), and another where it was cropped by 10% along the tag frame (d,e). These findings reinforce the adaptability of SIFT compared to other method used to identify and grant the originality of PUFs, making it a highly effective tool for authentication under varying imaging conditions.

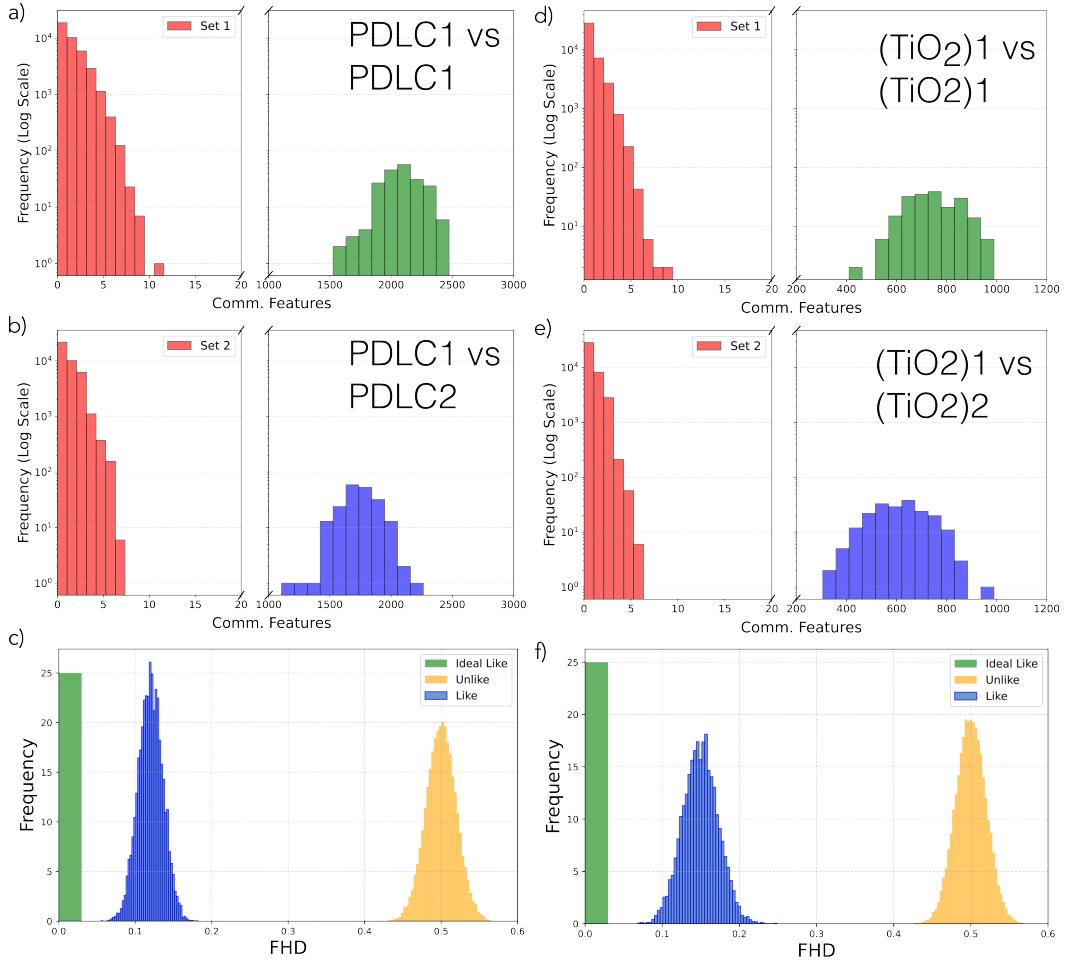


FIG. 6. SIFT applied to CRPs from the same dataset (PDLC1, (TiO<sub>2</sub>)1) and between two dataset collected at two different time (PDLC2, (TiO<sub>2</sub>)2) on a,b) the PDLC and d,e) the TiO<sub>2</sub> PUF. In the histogram the speckles that found their match are reported in green (same dataset) and in blue (for different dataset) while the other with no match are reported in red in both cases. c,f) Report the FHD for both PUFs typologies displaying the "ideal like" the analogue of SIFT green histogram, "like" (the analogue of SIFT blue histogram) and "unlike" distributions.

To further demonstrate SIFT ability to analyze speckle patterns generated by different types of optical PUFs, possessing different refractive index contrast and scattering strengths, we applied both the SIFT (using the same SIFT parameters) and FHD methods to PDLC and TiO<sub>2</sub> PUFs. Also for this analysis, a representative dataset of 200 speckles was used. We refer to this as PDLC1 and (TiO<sub>2</sub>)1 respectively. As reported in **Figure 6a,d**, for both

CPU model	number of CPUs RAM Gb	Single Core time (seconds)	Multi Core time (seconds)
Intel Xeon E5	4 64	83	30
Apple Silicon M1	8 16	40	15
Apple Silicon M3 - M4	11 - 10 18 - 16	19 - 18	7 - 7
Intel i7 10700	8 80	45	21
Intel Xeon Platinum 8358 (HPC Leonardo)	32 512	106	5

typologies, we obtained the same behavior of PS-PUF previously tested. However, it is worth noting that for the PDLC-PUF the number of matched recognized points is more than doubled with respect to PS-PUF ranging, now, between 1500- 2500 points. This is because more scattering particles (LC molecules for this PUF) are present in the volume of the analyzed PUF, producing more well-defined speckle grains into the speckle patterns, hence increasing the number of features that can be recognized and matched in the algorithm execution. In contrast, for the TiO<sub>2</sub>-PUF, the number of matched recognition points is approximately 800–1000, despite the high density of scatterers. This reduced number is attributed to the low transparency of the PUF having an OT=2.25, which lowers the contrast of the speckle grains in the collected images. Nevertheless, even with fewer points and reduced contrast, the SIFT based authentication is validated also for strongly scattering systems without the need of a fine tuning of the algorithm parameters. We can thus apply this methodology to a wide variety of optical PUF systems that can be adapted to a wide variety of applications and environments. The SIFT analysis is then performed on two datasets of the same PUFs collected at two different times referred as PDLC1,2 for PDLC and (TiO<sub>2</sub>)1,2 TiO<sub>2</sub>-PUF respectively. As expected, also for these PUFs, the number of matched features is maximized only for the 200 speckle patterns ( $R_i$ ) produced from the same challenge ( $C_i$ ) as indicated by the blue bars in Figure 6b,e. Instead, for all the other cases, only a few points are matched, namely false positive, as indicated by the red bar. As a counterproof, the FHD analysis has been performed on these datasets, see Figure 6c,f. The PDLC presents a "like" distribution peaked at 0.12 and TiO<sub>2</sub> at 0.15, while the "unlike" distribution is centered at 0.5 for both PUFs which is in agreement with the results of PS-PUF.

Finally, we improved the SIFT algorithm to work with multiple-processors to parallelize its operations and make it even more suitable in real and industrial applications [36, 37]. We performed a test comparing a selected speckle with a database of 1000 responses using workstations, laptops and a High Performance Computer HPC (the latter provided by Cineca). The results, reported in **Table III**, demonstrate the speed of operation of the proposed SIFT method to recognize the target response in a large dataset. The time ranges from 18/19 sec for Apple Silicon M3 and M4 to 106 sec for HPC Leonardo in single core while for multi-core operation, the time is dramatically reduced down to 5 sec using HPC to 30 sec using workstation CPUs Intel Xeon E5. This means that each single verification requires 5 microseconds, improving of 6 orders of magnitude the results reported in [27]. This test proves the easiness in implementing the proposed method in industrial applications.

#### IV. CONCLUSION

We present a straightforward approach to analyze the uniqueness of speckle patterns by using image recognition SIFT algorithm for optical PUFs authentication. To benchmark its performance, we compared SIFT results with the Fractional Hamming Distance (FHD) method. Both methods were applied to various types of optical PUFs, including those made from dielectric nanospheres (polystyrene and TiO<sub>2</sub>) and polymer-dispersed liquid crystals (PDLC). Our analysis highlights SIFT ability to extract and recognize several hundred unique features per speckle pattern. This capability even when comparing challenge-response pairs (CRPs) collected at different times and when identifying a target speckle pattern within a database. To demonstrate robustness, we applied the SIFT method to speckle images that were rotated, scaled, and cropped, achieving successful recognition in all cases. Additionally, the method supports real-time implementation as fast as 5 microseconds for each iteration using a multi-CPU setup. Overall, the proposed approach offers a fast, reliable, and scalable solution for both industrial and individual authentication systems, paving the way for effective anti-counterfeiting technologies based on optical PUFs.

## AUTHOR CONTRIBUTION

S.N fabricated and morphologically characterized the PUFs, G.E.L, F.R. and S.N settled up the experimental CRPs apparatus and acquire the data, G.E.L, M.D.L.B. and A.F. analyzed the data. G.E.L and A.F. conceived the idea and coordinated the overall research effort. The manuscript was written by G.E.L, M.D.L.B., S.N. and A.F with the input from all the authors.

## ACKNOWLEDGMENTS

G.E. Lio acknowledges the CINECA award (ID:HP10C1D8RJ) under the ISCRA initiative, for the availability of high performance computing resources and support. M.D.L.B, S.N. and A.F. acknowledge the financial support from project “PRIN 2022 2022T3B4HS-PE11 - Multi-step optical encoding in anticounterfeiting photonic tags based on liquid crystals (PHOTAG)” financed in the framework of Piano Nazionale di Ripresa e Resilienza (PNRR). F.R. acknowledges the project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU and cofunded by the European Union - NextGeneration EU, ”Integrated infrastructure initiative in Photonic and Quantum Sciences” - I-PHOQS [IR0000016, ID D2B8D520, CUP B53C22001750006]

- [1] J. W. Goodman, Some fundamental properties of speckle, *JOSA* **66**, 1145 (1976).
- [2] J. C. Dainty, *Laser speckle and related phenomena*, Vol. 9 (Springer science & business Media, 2013).
- [3] Y. Dong and B. Pan, A review of speckle pattern fabrication and assessment for digital image correlation, *Experimental Mechanics* **57**, 1161 (2017).
- [4] K. Basak, M. Manjunatha, and P. K. Dutta, Review of laser speckle-based analysis in medical imaging, *Medical & biological engineering & computing* **50**, 547 (2012).
- [5] J. Senarathna, A. Rege, N. Li, and N. V. Thakor, Laser speckle contrast imaging: theory, instrumentation and applications, *IEEE reviews in biomedical engineering* **6**, 99 (2013).
- [6] A. Pino, J. Pladellorens, and J. Colom, Method of measure of roughness of paper based in the analysis of the texture of speckle pattern, in *Speckle 2010: Optical Metrology*, Vol. 7387 (SPIE, 2010) pp. 560–566.
- [7] N. Farid, Speckle metrology in dimensional measurement, in *Handbook of Metrology and Applications* (Springer, 2023) pp. 1319–1345.
- [8] V. Tornari, On development of portable digital holographic speckle pattern interferometry system for remote-access monitoring and documentation in art conservation, *Strain* **55**, e12288 (2019).
- [9] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical one-way functions, *Science* **297**, 2026 (2002).
- [10] M. S. Kim, G. J. Lee, J. W. Leem, S. Choi, Y. L. Kim, and Y. M. Song, Revisiting silk: a lens-free optical physical unclonable function, *Nature Communications* **13**, 247 (2022).
- [11] H. Cao and Y. Eliezer, Harnessing disorder for photonic device applications, *Applied Physics Reviews* **9** (2022).
- [12] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, A puf taxonomy, *Applied physics reviews* **6** (2019).
- [13] Y. Wan, P. Wang, F. Huang, J. Yuan, D. Li, K. Chen, J. Kang, Q. Li, T. Zhang, S. Sun, *et al.*, Bionic optical physical unclonable functions for authentication and encryption, *Journal of Materials Chemistry C* **9**, 13200 (2021).
- [14] A. Ferraro, G. E. Lio, M. D. L. Bruno, S. Nocentini, M. P. De Santo, D. S. Wiersma, F. Riboli, R. Caputo, and R. C. Barberi, Hybrid camouflaged anticounterfeiting token in a paper substrate, *Advanced Materials Technologies* **8**, 2201010 (2023).
- [15] S. Nocentini, U. Rührmair, M. Barni, D. S. Wiersma, and F. Riboli, All-optical multilevel physical unclonable functions, *Nature Materials* **23**, 369 (2024).
- [16] F. Bin Tarik, A. Famili, Y. Lao, and J. D. Ryckman, Robust optical physical unclonable function using disordered photonic integrated circuits, *Nanophotonics* **9**, 2817 (2020).
- [17] G. E. Lio, S. Nocentini, L. Pattelli, E. Cara, D. S. Wiersma, U. Rührmair, and F. Riboli, Quantifying the sensitivity and unclonability of optical physical unclonable functions, *Advanced Photonics Research* **4**, 2200225 (2023).
- [18] S. U. Hussain, M. S. Riazi, and F. Koushanfar, Shaip: Secure hamming distance for authentication of intrinsic pufs, *ACM Transactions on Design Automation of Electronic Systems (TODAES)* **23**, 1 (2018).
- [19] M. A. Usmani, S. Keshavarz, E. Matthews, L. Shannon, R. Tessier, and D. E. Holcomb, Efficient puf-based key generation in fpgas using per-device configuration, *IEEE Transactions on very large scale integration (VLSI) systems* **27**, 364 (2018).
- [20] J. Daugman, The importance of being random: statistical principles of iris recognition, *Pattern recognition* **36**, 279 (2003).
- [21] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, *et al.*, Imagenet large scale visual recognition challenge, *International journal of computer vision* **115**, 211 (2015).
- [22] D. G. Lowe, Object recognition from local scale-invariant features, in *Proceedings of the Seventh IEEE International Conference on Computer Vision* (: Kerkyra, Greece, 1999) p. 1150–1157 vol.2.

- [23] D. G. Lowe, Distinctive image features from scale-invariant keypoints, *Int. J. Comput. Vis.* **60**, 91 (2004).
- [24] M. Bicego, A. Lagorio, E. Grossi, and M. Tistarelli, On the use of sift features for face authentication, in *2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)* (IEEE, 2006) pp. 35–35.
- [25] G. Badrinath and P. Gupta, Palmprint verification using sift features, in *2008 First Workshops on Image Processing Theory, Tools and Applications* (IEEE, 2008) pp. 1–8.
- [26] W. Burger and M. J. Burge, Scale-invariant feature transform (sift), in *Digital Image Processing: An Algorithmic Introduction* (Springer, 2022) pp. 709–763.
- [27] C.-H. Yeh, P.-Y. Sung, C.-H. Kuo, and R.-N. Yeh, Robust laser speckle recognition system for authenticity identification, *Optics express* **20**, 24382 (2012).
- [28] A. Ferraro, M. D. L. Bruno, G. Papuzzo, R. Varchera, A. Forestiero, M. P. De Santo, R. Caputo, and R. C. Barberi, Low cost and easy validation anticounterfeiting plasmonic tags based on thin films of metal and dielectric, *Nanomaterials* **12**, 1279 (2022).
- [29] M. D. L. Bruno, E. Fuoco, G. Petriashvili, G. Papuzzo, A. Forestiero, S. Sinopoli, U. Emanuele, R. C. Barberi, and M. P. De Santo, Cholesteric liquid crystals based micro-fingerprints generator for anti-counterfeiting labels, *Advanced Materials Technologies* **8**, 2300613 (2023).
- [30] S. Kamwe Sighano, T. Ritacco, M. D. L. Bruno, O. Gennari, W. Fuscaldo, D. C. Zografopoulos, J. Marae-Djouda, T. Maurer, R. Beccherelli, R. Caputo, *et al.*, Optical and terahertz anticounterfeiting tags via non-deterministic deposition of fluorescent opuntia ficus-indica extract, *Advanced Functional Materials* **34**, 2406632 (2024).
- [31] C. Champod and P. Chamberlain, Fingerprints, in *Handbook of Forensic Science* (Willan, 2013) pp. 57–83.
- [32] M. D. L. Bruno, G. E. Lio, A. Ferraro, S. Nocentini, G. Papuzzo, A. Forestiero, G. Desiderio, M. P. De Santo, D. S. Wiersma, R. Caputo, *et al.*, Flexible physical unclonable functions based on non-deterministically distributed dye-doped fibers and droplets, *ACS Applied Materials & Interfaces* **16**, 37063 (2024).
- [33] J. Wu, Z. Cui, V. S. Sheng, P. Zhao, D. Su, and S. Gong, A comparative study of sift and its variants, *Measurement science review* **13**, 122 (2013).
- [34] A. A. Sima and S. J. Buckley, Optimizing sift for matching of short wave infrared and visible wavelength images, *Remote Sensing* **5**, 2037 (2013).
- [35] Y. Wang, Y. Liu, Z. Xu, Y. Zheng, and W. Hong, Approximated scale space for efficient and accurate sift key-point detection, in *The Proceedings of the International Conference on Sensing and Imaging, 2018 2* (Springer, 2019) pp. 31–40.
- [36] Q. Zhang, Y. Chen, Y. Zhang, and Y. Xu, Sift implementation and optimization for multi-core systems, in *2008 IEEE international symposium on parallel and distributed processing* (IEEE, 2008) pp. 1–8.
- [37] J. Yang, J. Huang, Z. Jiang, S. Dong, L. Tang, Y. Liu, Z. Liu, and L. Zhou, Sift-aided path-independent digital image correlation accelerated by parallel computing, *Optics and Lasers in Engineering* **127**, 105964 (2020).