ADVANCED MATERIALS TECHNOLOGIES
www.advmattechnol.de

Smartphone Authentication of Unclonable Anticounterfeiting Labels based on a Microlens Array atop a Microphosphor-Doped Layer

*Vinay Kumar, Fabrizio Gota, Julien Neyret, Ngei Katumo, Aditya Chauhan, Stephan Dottermusch, Bryce S. Richards, and Ian A. Howard**

A phosphor-particle-loaded microlens array on a polymer substrate offers an attractive unclonable anticounterfeiting label design. A random pattern of bright emission points is created due to the random coincidences of light focused by a microlens with an underlying phosphor microparticle. The change of the bright point patter with the angle of the incident light (owing to a shift in the locations of the focal points) makes the labels unclonable. This work examines the authentication of such labels using a single smartphone. The smartphone flashlight provides illumination whereas the camera is used for detection (optical filters prevent capture of scattered source light). A 196-bit binary string is created from the captured images to identify which lenses in the 14 × 14 array create bright emission points for a given position of the smartphone. The classification of test and reference images as matching or not is achieved with >99% confidence, as is a 1 cm tolerance for the positioning accuracy of the smartphone. Moreover, authentication is possible for different distances between flash and camera provided this is less than 3 cm. In summary, the present work quantifies the good potential of the microlens array microphosphor unclonable label concept for authentication using a smartphone.

1. Introduction

Counterfeiting is a societal threat that poses both economic and safety problems. The Organization of Economic Co-operation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) stated in 2022 that the total cost of counterfeit goods to the international market in 2013 was about USD 1 trillion. It is expected to grow to more than USD 3 trillion by 2022–2023, amounting to >3% of global trade.[1] Beyond economic losses, counterfeit products can have a negative impact on human health. For example, nearly 60 million counterfeit respirators were seized across the globe during the COVID-19 pandemic.[2]

There is an increasing trend to identify products with unclonable labels to combat counterfeiting. In this approach, each individual product is marked with a unique label whose properties are characterized after manufacture. The uniqueness and unclonability of a label are based on some form of randomness in the manufacturing process, which is inherently impossible to control or reproduce. Each label possesses a nonalgorithmic unique pattern analogous to a human fingerprint.[3] Each label's unique pattern is characterized (by an appropriate method) after fabrication, and a digital representation thereof is stored in a database for retrieval and authentication.[4] The majority of such characterization relies on microscopy, as randomness on the micron scale is currently a robust method of ensuring practical unclonability. Once a marked product enters the supply chain, a range of actors up to the end consumers can authenticate the product by scanning the label and comparing the image against the reference. The simpler the hardware requirements for validation, the more accessible the authentication, and the technology becomes more commercially relevant. Hence, unclonable labels that can be verified using a smartphone are of prime interest, and recent systems have demonstrated that a smartphone with a clip-on magnifying lens can be used for authentication.[5]

In our previous work, we have introduced unclonable labels wherein the micron-scale randomness can be imaged with a standard camera (without any magnification lens). These labels are based on a microlens array on top of a polymer layer containing inorganic microphosphor particles.[6] The labels are illuminated through the microlens array, which causes the incoming light to be focused within the microphosphor-doped layer (in a small volume under each of the lenses). If the

V. Kumar, F. Gota, J. Neyret, N. Katumo, A. Chauhan, S. Dottermusch, B. S. Richards, I. A. Howard
Institute of Microstructure Technology
Karlsruhe Institute of Technology
Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen, Germany
E-mail: ian.howard@kit.edu

B. S. Richards, I. A. Howard
Light Technology Institute
Karlsruhe Institute of Technology
Engesserstrasse 13, 76131 Karlsruhe, Germany

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/admt.202201311.

DOI: 10.1002/admt.202201311

focal volume overlaps with a phosphor microparticle, then the resulting emission creates a bright point. These bright point patterns can be observed using a standard camera and lens (such as that found in a smartphone). To reproduce one such bright point pattern would be easy, e.g., by ink-jet printing an appropriate 2D pattern of phosphor. However, in this label design, the focal volume shifts depending on the angle of incidence (AOI) of the incoming light. Hence, for the same label, different bright point patterns are observed with different AOIs. So to authenticate a label of our design, one can require that a number of test images taken by a user under multiple different illumination conditions be considered matching with the appropriate reference images taken at the time of manufacture. As discussed below, at least two out of three test-reference comparisons should be deemed matching for the label to be classified as authentic. For a test and reference image from the same label to be deemed matching, the illumination conditions under which the test image is taken must also match (within some tolerance) those under which the reference image was taken. We previously found that the AOI tolerance, the maximum difference in AOI between the reference and test image for which the two would still be deemed matching, could be up to 3.6°.[7]

The results discussed above were based on labels designed to function in transmission mode, meaning that the illumination and detection are performed on opposite sides.[6] In this work, we examine how a single smartphone can be used to provide both illumination and detection on the same side. With a redesigned label (larger interlens spacing) and a simplified authentication algorithm (assigning a binary value to each microlens based on whether its focus leads to bright emission or not), we demonstrate that a single smartphone on the front side of the label can be successfully used for authentication. Two optical filters are still needed: i) a short pass filter to limit the wavelengths present in the smartphone's flashlight for excitation; and ii) a long pass filter to limit the wavelengths observed by the camera. In the old label design, the position of the camera at the back side was not important, as a change in camera position only resulted in a tilted projection of the bright point pattern, which could be corrected easily in the software algorithm for comparison. However, with front-side detection, as a significant fraction of the emitted light passes back through a microlens, the position of the camera relative to the excitation light-emitting diode (LED) becomes important. We investigate this issue but determine that for our label design the distance between the LED and the camera can vary up to a maximum of 3 cm without precluding authentication. Therefore, test images taken from smartphones with varying LED camera distances can still be deemed matching with reference images taken with a short (1 cm) LED–camera distance. This implies that one set of reference images taken at the time of manufacture can be used for comparison with test images taken irrespective of the smartphone used. The above analysis is done on microlens arrays fabricated in a UV-curable polymer on a thin glass layer that is then laminated onto a polydimethylsiloxane (PDMS) layer sparsely doped with microparticles. Such a design is useful for rapid prototyping of the label concept, but not suitable for applications. In this direction, we also introduce fully PDMS labels loaded with luminescent downshifting phosphor, wherein the PDMS microlenses are directly created in the doped PDMS layer. These flexible, 1 mm thick labels are qualitatively characterized to demonstrate potential routes to practically applicable designs of this label concept.

Recently, several important works relating to optically read unclonable labels have been published. Wu et al. presented unclonable labels based on random patterns of structural colors, created by injection casting of colloidal crystals.[8] For authentication, these structural color labels were analyzed using point-by-point scanning to measure the reflectance spectrum using a USB spectrometer. Liu and co-workers investigated how crystallization and the Ostwald-ripening process of perovskite crystals within a single inkjet drop can lead to unclonable patterns detectable by microscopy.[9] Kim et al. reported unclonable labels based on silk with the proper density for the random pinholes to lead to self-focusing points on a detector plane.[10] In this system, silk "identification cards" could be characterized by placing them on top of an image sensor and recording the patterns generated by various wavelengths of light. Torun and co-workers demonstrated that random microscale structures could be created by the de-wetting of thin polymer layers caused by thermal annealing.[11] This simple process leads to complex microstructures that can be characterized by microscopy, or other methods based on the introduction of appropriate taggants to the islands.[11] Similarly, Kayaci and co-authors demonstrated that organic light-emitting materials could be used to create robust anticounterfeiting labels based on photoluminescence images.[12] Esidir et al. reported that electro-spraying could be used to create polymer mats with unique morphologies and properties that could be used as a basis for anticounterfeiting.[13] A paper by Wang et. al. detailed unique unclonable labels, realized via observing (with fluorescence microscopy) the complex rings of color at the edges of microscale "sky-domes" containing a few dye-doped droplets.[14] These works all demonstrate how characterization of locations of micron-scale objects is an important paradigm for the generation of unclonable labels. Our label design has the unique and attractive feature that the microlens array creates a macroscopic, high-contrast image that is easy to capture and analyze but based on the precise locations of the micron-scale objects. Furthermore, the microlens array adds security to our label concept. For one of our labels to be reproduced, not only must all of the 3D locations of the microparticles within the host layer be reproduced to an accuracy on the order of 10 µm, so must the position of the lens array relative to this point cloud of particles. Otherwise, even if the particle positions were identically reproduced, the different placement of the microlens array relative to the particles would lead to different bright point patterns at given angles. So, the key advantages of our label concept are 1) that the micron-scale positions become able to be viewed easily on the macroscale in high-contrast images that are easy to analyze, and 2) that the measurement of a subset of the positions with each angle (selected by the microlens array) adds a further significant barrier to preclude the possibility of cloning a label.

An ideal authentication system should be able to employ ubiquitous and inexpensive technology such as smartphones. In this regard, the Sørensen group demonstrated that the random positions of scattering inorganic[5a] or polymer (beneficial for recycling),[5b] can be characterized with a clip-on smartphone lens to make unique anticounterfeiting labels. They have developed an unclonable label system wherein each of the three canvases created by the corner squares of a QR code can be authenticated with a smartphone application.[5a,b] In other approaches, the 2D pattern created by grain boundaries in block copolymer films were imaged with a smartphone with a clip-on lens by Wu et al. to make an anticounterfeiting label.[5c] These works illustrate how the recognition of random patterns based on smartphone images is rapidly progressing; the additional security of the change of bright point pattern with smartphone position in our labels (described below) adds an attractive layer of security to this approach.

2. Results and Discussion

We first introduce the label concept and excitation/detection geometry. We then discuss the label design and the fabrication process. The microlenses are originally made on a glass layer and laminated to a microparticle-doped PDMS layer. This glass-sandwich production proved dependable for initial optical verification. However, a latter route will demonstrate that all components can be replicated in PDMS. We detail the label-authenticating algorithm and make a qualitative and quantitative assessment in terms of authentication upon using a single smartphone for taking both the reference and test images. We then adjust the distance between the excitation LED and detection camera, to quantify how the labels perform when different smartphones are used for taking the original reference images and the test images.

2.1. Label Concept, Excitation, and Emission Geometry

Figure 1a shows a composite photograph of a smartphone reading out a bottle marked with one of our anticounterfeiting labels. Multiple images with different exposure times were taken and then combined into one high dynamic range (HDR) image to see contrast in parts of the scene with different lighting levels. A smartphone (Galaxy S20 5G, Samsung) illuminates the label (1 × 1 cm—more details later) with its flashlight through a 500 nm short pass filter (FES0500, Thorlabs). This leads to the blueish illumination color (the bottle is white under standard illumination). The scene is imaged by the smartphone camera that has a 500 nm long pass filter (FEL0500, Thorlabs) placed in front of it. The mechanism leading to the creation of a bright point is schematically presented in the inset of Figure 1b. As discussed below, the larger spacing of the microlenses allows each bright emission point to be associated with one microlens.

A simple binary code can be generated from this emission point-microlens association. The code is a string of the same length as the number of lenses in the array. A “1” corresponds to a bright emission under the focus of the given microlens. A “0” marks the absence of emission.

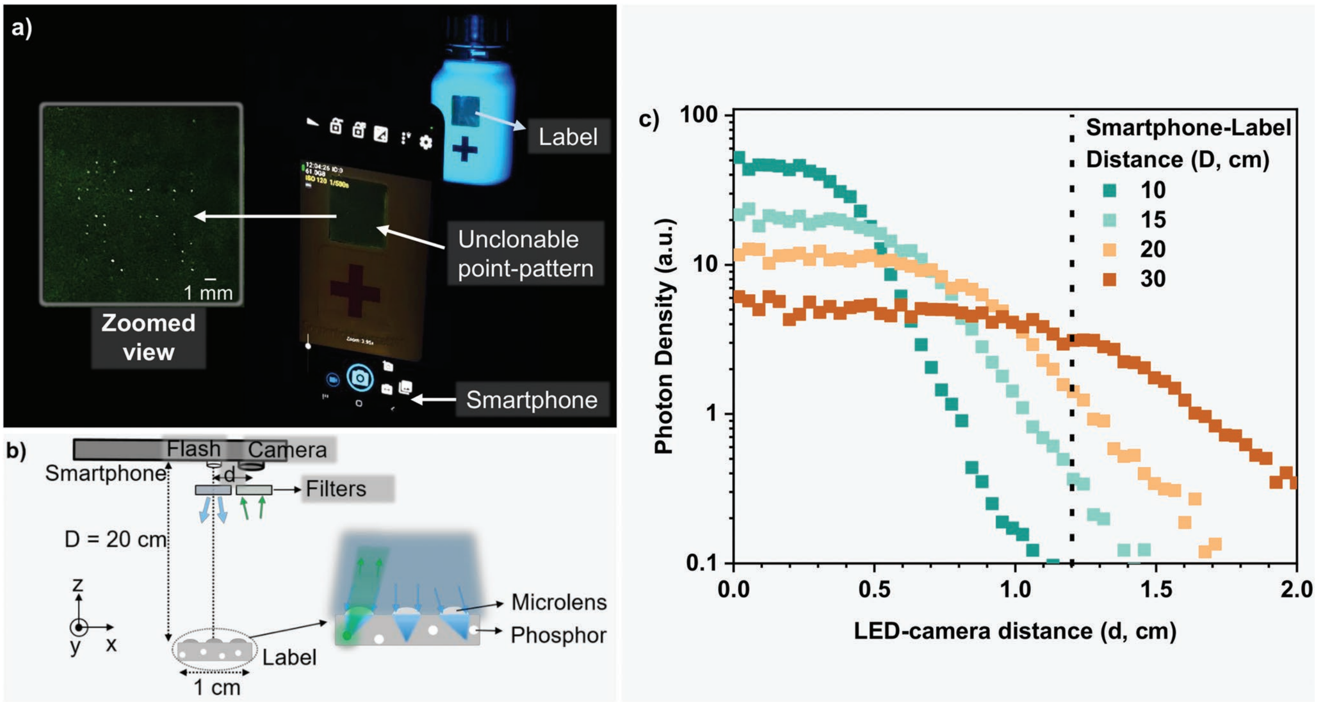

Figure 1. a) An HDR photograph of a smartphone authenticating a labeled product (captured in dark). The label is illuminated using the camera flashlight with a 500 nm short-pass filter attached to it. The emission of the dilute dispersion of phosphor microparticles under the microlens array is imaged by the smartphone camera through a 500 nm long-pass filter (to exclude excitation light). A zoomed view of bright point pattern from the label is shown in inset. b) A schematic of label-smartphone set up to observe the generated bright point pattern. A brighter emission point is created when incident light is focused onto a microparticle, and locations of such bright emission can be associated with given microlenses based on the image captured by the smartphone. c) Radially integrated photon density profile observed from an emission center (through microlens side) by the detector placed at different distances.

Figure 1b presents the geometry of the excitation and emission. The "origin" corresponds to the flashlight of the smartphone centered above the microlens array. The relative position of the smartphone and the label can be shifted in the direction labeled "y" via a translation of the smartphone. This relative change in position also affects the AOIs at the individual microlenses on the label. We note that the AOI varies for lenses across the label due to the point-source-like angular emission of the distant smartphone flashlight and the different angles from the flashlight to each lens array (as schematically illustrated in Figure 1b). Nonetheless, as the smartphone is moved, the AOI at each lens changes. In all the experiments below the smartphone is held at 20 cm from the label and the flashlight-to-camera distance is 1.2 cm for the smartphone model used.

As illustrated in Figure 1b, the emitted light must pass through the microlens to reach the detector (camera). This will lead to partial "collimation" of the emitted light by the microlens as the emitted light travels back up toward the detector. If the distance between the LED and camera is small, then the camera should capture this "beam" of partially collimated light. However, if the distance between the LED and camera is too large, then the camera will be outside the light beam and the bright point will be missed. The size of the beam expands with increasing distance between the smartphone and label (due to the nonperfect collimation). To get a zeroth-order estimation of whether a camera at a given distance from the flashlight will be able to pick up the bright light created under a microlens at a given distance between the label and smartphone, we perform ray-tracing simulations using pvtrace (see Supporting Information, Section S2 for details).[15] For the simulation, a lens of the geometry defined in the label fabrication section below is implemented and a round emitter of 30 µm diameter (matching the size of the microparticles used) is placed at the focal length under the lens directly at its center (Figure 1c). The virtual detector screens are placed at 10, 15, 20, and 30 cm from the label surface to record the distribution of emitted light at these distances. The 2D distribution of photons on these screens is displayed in the Supporting Information (Figure S3, Supporting Information), and the radially integrated photon density as a function of LED–camera distance is plotted in Figure 1c (the center to the distribution corresponds to the position of the flashlight due to reciprocity). At 20 cm distance between the smartphone and label, more than 10% of the maximum intensity will still be captured by a camera 1.2 cm away from the flashlight. Although moving to 30 cm would increase the acceptable distance between flashlight and camera, we found the excitation intensity of the smartphone flashlight becomes too weak to effectively excite the phosphors. We therefore choose a 20 cm smartphone-label distance for the work presented herein, although the Supporting Information also provides an experimental consideration of how a variation in smartphone label distance affects authentication.

We note that this simple raytracing analysis does not account for the following: i) the scattering surfaces; ii) not all bright emission will come from exactly the focal plane of the lens; and iii) imperfections/surface roughness in the lens due to fabrication. All of these will decrease the "collimation" of the emitted light and allow larger LED–camera distances to still capture some of the bright points. This is experimentally confirmed later, that although the number of bright points captured drops off as the LED–camera distance increases, test images taken at a 3 cm LED–camera distance are still deemed matching with reference images taken at a 1 cm LED-camera distance (with the LED being held in the same location).

2.2. Label Design and Fabrication

We start with examining the smartphone-based authentication of a two-layer unclonable label, wherein a microlens array made on glass is laminated to a microphosphor-doped PDMS layer. Despite lacking robustness, flexibility, and long-term stability,[7] it does enable rapid prototyping and quantification of the label performance. The detailed fabrication procedure for such labels is provided elsewhere.[6] Briefly, a positive master of the microlens array is written into IP-S photoresist (Nanoscribe) using two-photon lithography (Photonic Professional GT, Nanoscribe). The selected substrate is ⟨100⟩ oriented silicon wafer which was anisotropically etched to expose ⟨100⟩ planes, resulting in a square-base pyramidal microtexture. This surface structure helps to outcouple light that does not travel through the microlenses and should slightly enhance front-side detection. The microlens array itself consists of spherical lenses with a focal length of 550 µm, a radius of curvature of 200 µm, and a base diameter of 250 µm spaced with a center-to-center distance of 750 µm in a 14 × 14 array. Once the positive master is created, a second negative master is made by replicating the positive master with PDMS. This PDMS negative master is used to stamp a thin layer of resin that is cured using UV light (NOA-88, Norland), which is placed on a 400 µm thick glass substrate. The microparticle-doped PDMS layer is then introduced under the 400 µm thick glass as follows. First, a commercial phosphor powder with a diameter (D50) of 32 µm (YYG-557-230 isiphor, Sigma-Aldrich) is introduced into a silicone elastomer base (SYLGARD 184, Dowsil, RTV-A) at 0.5 wt% and dispersed with a high-speed dispersion device (CAT M., Zipperer GmbH). Then, the curing agent (RTV-B) is mixed throughout the solution with a component ratio RTV-A:RTV-B of 10:1. The resulting solution is kept in a vacuum desiccator to extract dissolved air from the mixture and then poured onto a glass slide between two strips of 200 µm thick tape. The 400 µm thick glass plate with the lenses on top is then pressed onto the PDMS and the sandwich structure is cured on a hotplate at 100 °C for 15 min.

2.3. Authentication Algorithm

Previously, we used an algorithm to determine and compare the 2D locations of the bright points in captured images for authentication.[6] In this earlier design, the lenses were close-packed and it was difficult to assign a bright emission point to a given lens. In the present approach, with the sparse spacing of the lenses, it is possible to associate a single bright point with a given lens, which allows the creation of a remarkably simple representation of the bright point image. Namely, the bright point pattern can be represented by a binary string whose length is equal to the number of lenses in the array. A fiducial mark is needed to indicate the orientation of the label (e.g., mark the top left of the array) to parse the lenses into a string in a consistent way. This results in a facile comparison of the reference and test strings, as the fraction of bright points that are in the same location can be easily determined. The individual steps to generate the strings from captured images are now presented in detail.

First, the label and smartphone are fixed in the desired position. We use a laser-cut holder to position the smartphone above the label and allow translation of the label in one direction (photograph of setup in Figure 1a). With the positions of the smartphone and label now fixed, an image is taken with background lighting on (**Figure 2**, step 1). A crop of the region of interest from the background light on the image is shown in Figure 2, step 2. Here, each of the lenses in the array is clearly visible and the center location of each lens can be determined. This is currently done manually by identifying the centers of the four lenses in the corners, but more sophisticated algorithms could fully automate this center-finding step. Once the centers are identified, a square array of touching circles is defined centered on each of the microlens (Figure 2, step 3). This array of circles is the red lines superimposed on the background light image. The red circles indicate the area of pixels that will be associated with each microlens. The background light is then turned off, the smartphone flashlight is turned on, and an image of the emission is taken. A representative image of the resulting emission is presented in Figure 2 (step 4). The image is cropped to the same pixels as that determined from the background on the image, and the red circles defining the region associated with each microlens (as previously determined) are again displayed. The application Open Camera (v1.48.1 Code: 77) is used to keep the ISO constant at 450 and the exposure time constant at 1/50 s. The white balance is also fixed as 7000 K. These acquisition conditions lead to images that are dark, with just a few bright points. To assign whether a lens is bright or dark, we consider an image made from the sum of the pixel values in the red and green channels over the same region of interest shown in the cropped image (step 2, Figure 2). The average pixel value was measured, and 1.5 times the average was subtracted from the whole leaving only the "spikes" corresponding to bright pixels (step 5, Figure 2). The sum of the pixel values in each lens area in this new image is computed, and a lens in which this sum exceeds 10 is considered to be a bright point. The raw images and the code used for generating this and all other Figures in this article can be accessed from the Gitlab repository (see Data Availability Statement Section for link).

This quick and robust method was used to assign a value for each lens. A string is then formed by placing these binary values in the order indicated, starting from the top left of the label (identified using the visible fiducial mark).

To assess the similarity of two-point patterns, we calculate the fraction of the bright points in the two images that are acquired

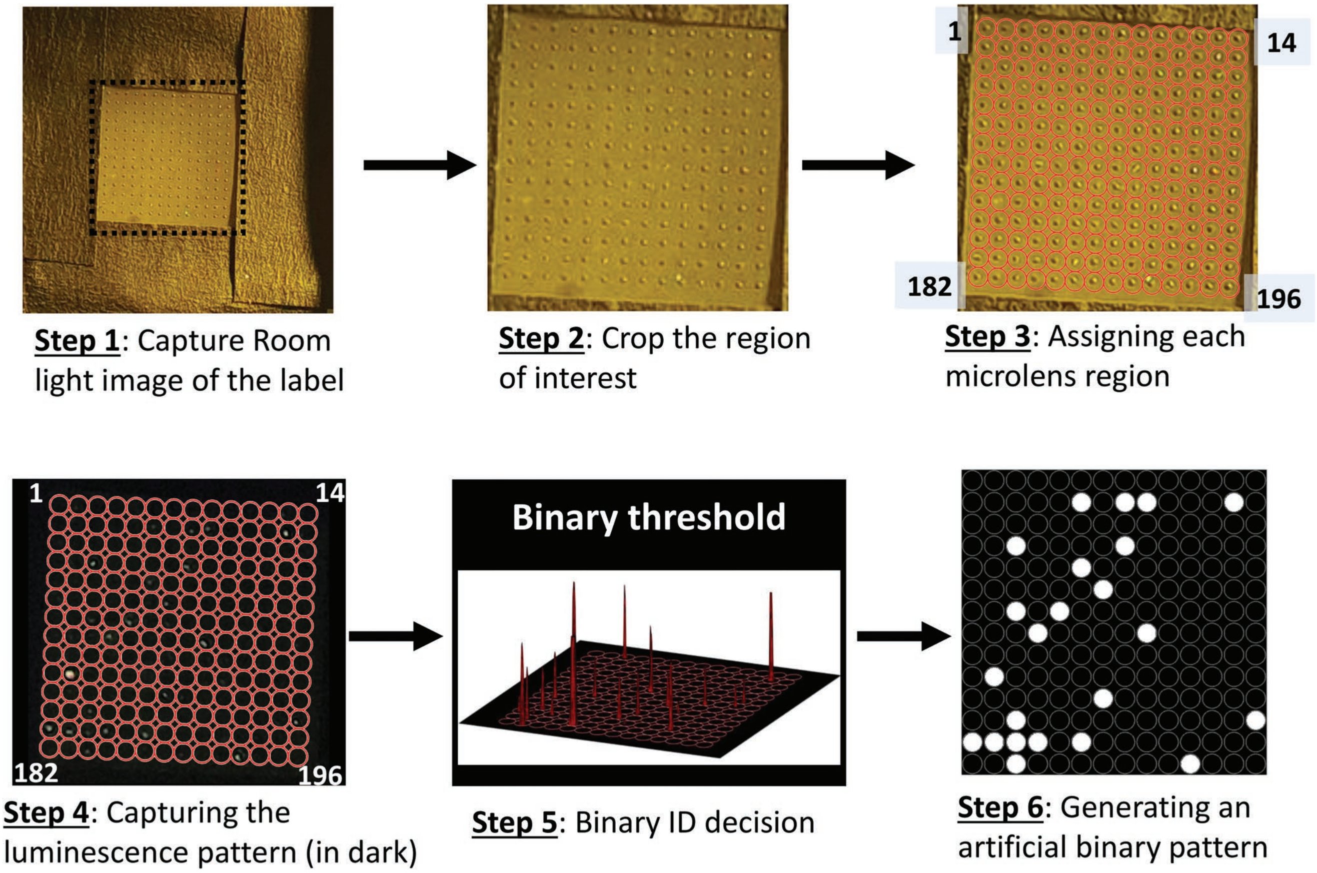
Step 1: Capture Room light image of the label
Step 2: Crop the region of interest
1
14
182
196
Step 3: Assigning each microlens region
1
14
182
196
Step 4: Capturing the luminescence pattern (in dark)
Binary threshold
Step 5: Binary ID decision
Step 6: Generating an artificial binary pattern

Figure 2. Algorithm to generate a binary string for assessing the state of every microlens as either a bright (1) or dark (0) point. An image is captured with background light on to assign locations of microlenses based on the fiducial mark. If 3 pixels within the region of a microlens are 1.5 times the average pixel value then the microlens is considered to have a bright point.

under the same setup (distance and AOI). First, we compute the total number of bright points in both images by summing up the number of 1s in both of the strings. This gives the total number of bright points (TB) in the reference AND test string. Then, the reference and test strings are added bitwise. When a 1 is present in the same place in the test and reference string, there will be a "2" in that location in the bitwise sum string. The number of twos in the bitwise sum sting is counted. This gives a value for the number of bright points that are in the same location in both test and reference images (SB). Then, the metric F is computed as the fraction of the total bright points in the two images that are in the same place. F is simply 2SB/TB. The value of F can vary from 0 (no bright points are in the same place in both strings) to 1 (all bright points are in the same place in both strings). As shown below, this is a good quantitative metric to use for comparing whether given test and reference strings match. For the interested reader, we note that F shows less variability in nonmatching cases than the Hamming distance and thereby allows a better classification decision.

To briefly discuss the possible number of unique codes generated by such a label, one can consider the following model. A 14 × 14 lens array can generate a binary string of length 196 where a given number of '1's be randomly distributed. With the current doping level (0.5 wt% of phosphor), on average around 25 bright points are observed which would lead to around $\binom{196}{25} = 10^{31}$ unique codes. Therefore, the conversion into the bit string still maintains enough information content to allow many unique labels to be created and keep the probability of creating identical labels vanishingly small.

2.4. Qualitative Analysis of Labels

We have described the algorithm to convert the bright point pattern images to a binary string. We now qualitatively go through the reproducibility, unclonability, and uniqueness of the binary strings produced.

1. *Reproducibility: multiple trials on a single label always replaced at the same position*—A single label is placed on the sample holder and a luminescence-based point pattern image is captured using the filters-equipped smartphone flashlight and camera. The label is repeatedly removed and re-inserted within the label stage, translated to a random position, then back to the home position to make different trials. For each trial, the luminescence-based pattern and the room light image of the label are captured. As presented in **Figure 3**a, we perform three different trials for a single label (named label 1 or L1). For easy visual comparison, the three resulting binary strings are illustrated in the same pattern as the lenses with dots in red (R), green (G), and blue (B), respectively. A composite image of the three different trails is also shown in a single frame image. Apart from a few minor fluctuations, most of the bright points obtained from the images of three different trials are overlapping, resulting in the generation of white dots (R + G + B → W) in the composite image. This serves as proof of the reproducibility of the point pattern from a given label.
2. *Unclonability: single label at varying position*—It would be easy to clone a single pattern of bright emission points from a label; a counterfeiter could print a fluorescent ink pattern that would spoof the bright point pattern created for a given label at a given position. However, the change of bright emission point pattern with the relative position of the phone and the label completely negates such approaches to counterfeiting. To demonstrate that a single label generates multiple different unique patterns, L1 is placed on the sample holder, and the smartphone is translated along the y-axis from 0 to 2.5, and then to 5.0 cm. The shift in the relative position of the smartphone and label causes a shift in the AOI, which induces a change of the focal volume under each lens. The strings generated for the new bright point patterns acquired at different distances are presented in red, green, and blue individually in Figure 3b. Creating a composite image of these images shows that different patterns are indeed generated upon the motion of the smartphone and therefore that the unclonability of the labels is strong. The interested reader is directed to a directly observable demonstration of how the bright point pattern changes as the smartphone is moved provided as a Supporting Video.
3. *Uniqueness: multiple labels fabricated*—To demonstrate that each fabricated label (with the same doping concentration of the phosphor) leads to a random bright point pattern, the strings generated for three different labels (taken at the home position of the phone) are displayed as red, green, and blue in Figure 3c. Again here, the composite image shows that the labels are unique, and each individual label has a unique constellation of bright points as a consequence of the random microparticle locations in the microparticle-doped film. We note that the randomness of the labels can be more quantitatively assessed by comparing the Pearson correlation coefficient between the patterns. As described in Section S3 of the Supporting Information, the absolute magnitude of the correlation coefficients between the patterns always lies below 0.2, supporting our expectation that each label instance leads to a unique and random emission pattern.

2.5. Quantitative Analysis of Labels

We need a large set of test and reference images with known pairs that should both authenticate and not authenticate to quantitatively assess the performance of these labels. To obtain these, we fabricate eight labels and image them at two different smartphone positions (y = 0 cm and 5.0 cm). After these reference images are taken, we then reinsert the labels and use the same smartphone to take a series of test images returning to the same relative positions as above. Given the point patterns taken for the same label at the different positions are uncorrelated (as suggested above and proven subsequently), this leads to 16 reference and 16 test images. Of the 256 comparisons of binary strings generated from this image set, 16 should authenticate whereas the remainder should not. To get a larger population (and thereby better statistics) for the "matching" reference-test images that should authenticate, we take an image of each label also at y = 2.5 cm. These images cannot be used to gather statistics for the nonmatching population, as they

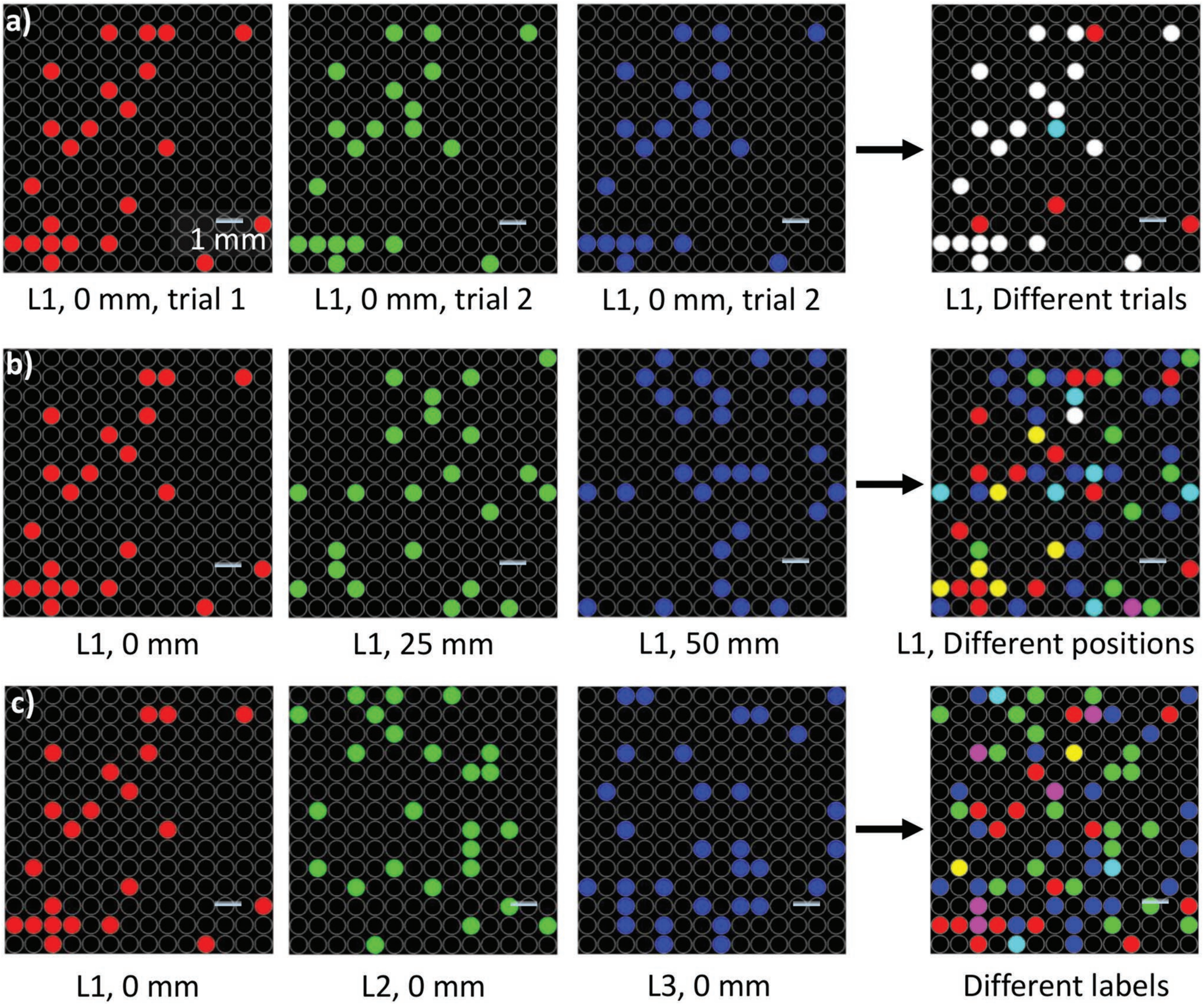

Figure 3. Representation of the binary strings measured for a) three different trials of the same label at the same position to show reproducibility. b) The same label at three different positions to show the bright point pattern changes with smartphone position demonstrating unclonability. c) Three different labels to show each label is unique. The first three images in each row show one string, whereas the composite image at the end of the row allows the similarity (or difference) of the strings to be visualized.

are still somewhat correlated with images taken 2.5 cm away from them (F is around 0.5 for comparing a reference taken at 0 cm and a test at 2.5 cm, e.g., much higher than the F for truly unrelated images). However, the reference and test images both taken at 2.5 cm are different from the ones taken at 0 and 5.0 cm, so can be used to add eight more cases to the "matching" population bringing its total up to 24. The full code used in the algorithm for comparison of reference-test images to generate **Figure 4**a,b is available at the repository mentioned in the Open Research Statement.

For the off diagonal (nonmatching) 256 reference-test image pairs, the value of F varies from 0 to around 0.35, with the mode being under 0.1. This histogram can be compared to the theoretical model histogram (presented in light blue). The theoretical histogram is generated by the code found in the Gitlab repository as addressed before. To generate the model histogram, 30 integers between 0 and 196 are chosen at random with repetition possible. We repeat the operation 10^6 times to generate the locations of bright points for 10^6 different labels. On average, 28 points will be bright on such a label (2 numbers of the 30 will be repeated draws of the same number). This agrees reasonably well with the number of bright points detected on average in our labels. Then, F is computed for 10^6 comparisons from this label population, and the histogram for these comparisons is presented. These distributions roughly agree, although the experimentally observed distribution is slightly broader—likely due to the slightly larger variation in the number of bright points between labels compared with the simple model calculations. Nonetheless, the agreement is sufficient for us to conclude that the observed distribution in F for the nonmatching population is consistent with the fraction of bright points occurring in the same location expected by random chance. Fitting a Gaussian probability density function (PDF) to the nonmatching population leads to a central position of 0.16, and a width (full-width at half-maximum (FWHM)) of 0.19. The corresponding cumulative density function (CDF) is shown as the dashed line and gives the total probability that F will be less than a given value for a nonmatching pair.

The histogram for the matching population (reference and test images should match) is displayed as the orange columns in Figure 4b. Satisfactorily, it is apparent that there is a large separation between the tight distributions in F for the nonmatching and matching populations. This means it will be possible to use F to accurately classify whether given reference and test images belong to the matching or nonmatching populations, and therefore should authenticate or not. The Gaussian PDF fit to the matching population suggests a center of 0.15 and width (FWHM) of 0.18. The CDF associated with the matching population is presented as the dashed orange line. This shows the total probability that F is above a given value for a comparison of images in the matching population.

We wish to select a threshold value for the F above which we consider the patterns to match (will lead to authentication), anything below this is considered as nonmatching. As can be seen, there is an excellent separation between the distributions for the F for the matching and nonmatching populations. To place the threshold within this gap, we consider the F value for which the CDFs cross. They cross at $F = 0.45$, with a value of more than 0.99. This means, choosing a threshold of 0.45 for authentication results in a probability of false positive (images authenticating when they should not) or false negative (images not authenticating when they should) less than 1%. This is attractive, as the computation of F is trivial and extremely quick (a single test-reference comparison in Matlab running on an Intel Core i5-3740 3.2 GHz chip took 100 µs). Thus, strategies that involve the testing of a few test images against many reference images are unproblematic to implement and could help circumvent some barriers to hand-held authentication as will be considered in the Conclusions section.

2.6. Tolerance of Classification to Smartphone Movement

In the previous section, we demonstrated that a single smartphone on the front side of the label manages to properly classify matching and nonmatching reference-test pairs taken at the same camera position. However, it is desirable that images will be considered matching when there is a slight change in smartphone position between the reference and test images, say less than 1 cm. This means that the tolerance with which the smartphone need be placed to take a test image is easily achievable with simple hardware (i.e., a holder in which the smartphone and label are placed by hand). However, to maintain the unclonability, a substantial change in position, say 5 cm, should lead to fully uncorrelated bright point patterns (this has already been demonstrated in Figure 4). In the following, we show that our label design indeed allows for this desired performance in terms of achieving 1 cm positioning tolerance.

To determine the tolerance of correct classification against difference in the smartphone position between the reference and test images, we translate the smartphone along one axis (y-axis) from $y = 0$ to 40 mm, with a step of 1 mm. The vertical distance of the smartphone to the label is maintained at a height of 20 cm. We then select each of the 11 images in the middle of this range to be reference images. For each of these reference images, there are test images with offsets relative to the reference image within ±15 mm at every mm. **Figure 5**a presents F for each of these 11 reference images versus the 31 test images with offsets spanning from −15 to 15 mm (the 0 offset test image is identical to the reference image and therefore always yields $F = 1$). We recall from Figure 4 that the threshold for F is 0.45, meaning green, yellow, and red colors in Figure 5a indicate reference-test pairs that will be considered a match. From −8 to 12 mm, the test images are considered to match with the reference images. This is confirmed in Figure 5b, wherein the probability of classification as a match is computed by the fraction of the 11 reference images that authenticate with a test image at a given offset. The width of the window in which

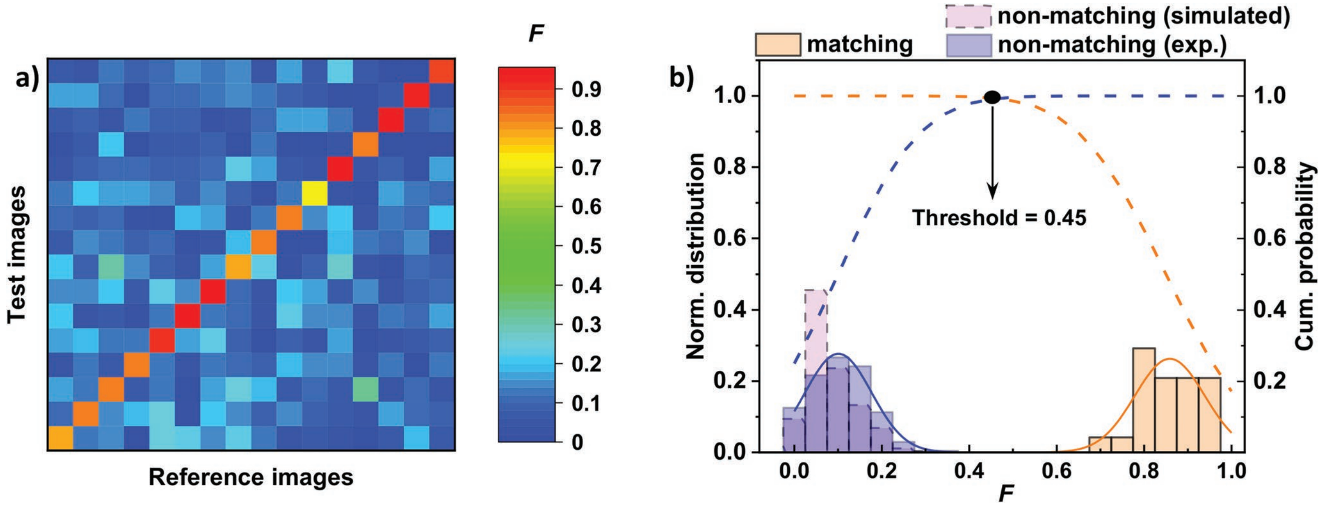

Figure 4. a) Fraction of bright points in the same location in the reference and test images, F, for test-reference image pairs in the matching population (diagonal) and nonmatching population (all other positions). b) Histograms for F in the matching and nonmatching populations with probability density functions estimated by fit to normal distribution (solid lines). Also, the corresponding CDFs (dotted lines) whose crossing point is used to select the threshold F above which reference and test images are considered matching.

classification as a match is "certain" (all 11 trials authenticate) is 2 cm. This roughly means that as long as the smartphone is not displaced by more than 1 cm from the position, it was in when the reference image was taken, then classification will work.

The slight asymmetry of this window is due to the geometry of the problem. The AOIs on the microlens change quickest with the motion of the smartphone as the smartphone is moved away from the "home" position centered on top of the lens array. A 1 mm offset from this home position leads to a more rapid change in focal point positions than a 1 mm change when the smartphone is already, e.g., 1.5 cm away. Thus, the tolerance is the smallest for the reference images with the smallest numbers moving to negative offsets. These situations correspond to a starting position just 1.5 cm (or slightly above) from home, then moving back to the home position, i.e., covering the region wherein the shift of the focal volume with position will be the greatest. To summarize, the results of Figure 5 demonstrate that a tolerance to smartphone motion between the reference and test images of 1 cm is achievable with the current design. This is already a positive result and confirms that hand positioning of the smartphone and label with simple markers is sufficient to reproduce the same geometry as the reference image within the 1 cm tolerance. The asymmetry in Figure 5a,b is a consequence of the focal volume shifting more rapidly with smartphone motion when the smartphone is near the current "home" position. Therefore, for a practical application, it could be desirable to purposefully demand test images with a larger offset from the home position as the tolerance for misplacement of the smartphone with respect to the reference will be slightly greater in these cases.

2.7. Tolerance of Classification to Different LED–Camera Distances

Until now, all results presented were made using a single smartphone. One other important consideration is that different smartphones have different locations of the camera relative to the LED flashlight. We need to assess whether different LED–camera distances affect the correct classification of test images. For backside detection, the position of the camera is known to be unimportant.[6] This is not necessarily the case for frontside detection, as demonstrated theoretically for a perfect lens and without scattering structure in between lenses in Figure 1c. This partial collimation leads a bright point's emission to be observable only for some subset of LED–camera distances. As the LED–camera distance increases, the probability of catching the emission from a bright point on the camera will decrease.

To test this experimentally, we use the setup depicted in **Figure 6**a. An external white LED (CXA1304 LED, Cree Xlamp) is mounted at a fixed position (1.0 cm offset from the "home" position) and used for excitation. The smartphone is mounted on a translation stage so that the position of its camera can be translated from a minimum offset (d) of 1.0 cm from the external LED to a maximum offset of 6 cm. Images are taken as the smartphone is translated in steps of 1 mm.

Figure 6a is a schematic of the experimental setup used to characterize the dependency of the bright point pattern observed as a function of the LED–camera distance. The bright point pattern measured at 1, 2, and 3 cm LED–camera offsets is shown in the red, green, and blue strings in Figure 6b. Here, we can visually note that, as expected, the number of bright points decreases as the LED–camera distance increases. This is confirmed quantitatively in Figure 6c, where the number of bright points detected in an image steadily decreases from around 40 at a 1 cm LED–camera separation to only 10 at a 6 cm LED–camera separation. Fortunately, although bright points drop out of the pattern as the LED–camera separation increases, the remaining visible points have the same position. This can be seen in the composite image in Figure 6b. 13 white (bright) points remain in every image, while the additional 4 yellow points that are still present at 2 cm disappear at a 3 cm offset. Taking the 2 and 3 cm patterns as test strings and the 1 cm pattern as the reference image leads to the fraction of total bright point positions matching, *F*, being 0.6 and 0.5, respectively, which is still above the threshold of 0.45 for considering the strings matching. Thus, these patterns qualitatively indicate that correct classification can be achieved when reference images taken at a 1 cm LED–camera distance are used even for test images taken with larger LED–camera distances.

For a more quantitative view of how *F* decreases with increasing LED–camera separation, the test images taken at each mm step are compared to the reference image taken at a 1.0 cm separation. The results are presented in Figure 6c, and although *F* decreases steadily, it stays above 0.45 until an LED–camera separation of 3.3 cm. Thus, our results indicate that a single reference image is sufficient for the correct authentication of a test image taken on a variety of smartphones if the LED–camera distance is less than 3 cm. We are unaware of any smartphone with an LED–camera distance of greater than 3 cm, indicating that all smartphones would allow authentication of our labels.

2.8. All PDMS Labels

As a final experimental direction, we show that it is possible to produce flexible, all-polymer-based labels. For this, the same label design is used but a negative master is created on a nickel shim (from a positive replication in NOA, details in the Supporting Information, Section S3). A photograph of this negative master on the nickel shim is shown in **Figure 7**a. Then phosphor-loaded RTV-A component is mixed with the RTV-B component, degassed, and poured onto the nickel shim with a small frame used to control the thickness to 1 mm. This is then degassed for 10 min and heated to 120 °C for 10 min on a hotplate. At this point, the pure PDMS label can be carefully detached from the shim. A photo of such a single layer, flexible PDMS layer is presented in Figure 7b, and more fabrication details are given in the Supporting Information.

Figure 7c presents the qualitative comparison of point patterns obtained for these single-layer labels, demonstrating that they are equivalent to the PDMS-glass hybrid prototypes that were used in the previous sections. We also note that the label imaged in Figure 1a as an example of an on-good application is made from this single-layer PDMS design. The *F* value estimated for the qualitative analysis of trials (test images) is >0.9, indicating excellent

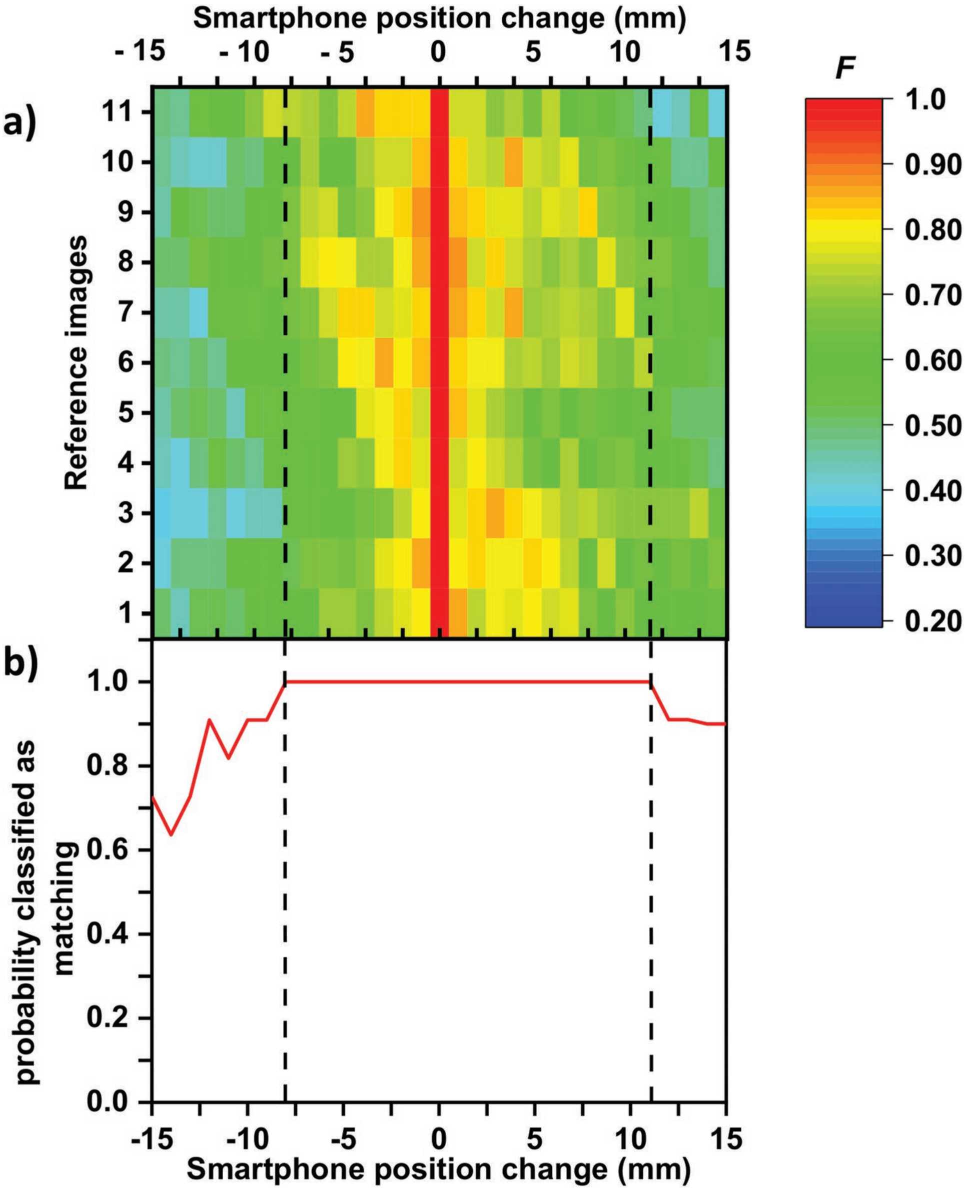

Figure 5. a) Comparison of the normalized number of same bright points of reference-test image pairs as the smartphone is translated. 11 references images are considered, with 30 test images taken at varying offsets in the smartphone position for each reference image. b) Authentication probability as a function of offset in smartphone position between reference and test image derived from data in (a). The label will authenticate if offset is less than 0.95 cm.

reproducibility of patterns. Whereas, for different patterns (under different smartphone positions and for different labels), F lies <0.3 showing the uniqueness of luminescence patterns from the labels. To make an initial assessment of the stability of these labels, we place them in an environmental chamber normally used for testing solar cells. Here, they are constantly exposed to simulated sunlight and held at the elevated temperature of 80 °C. As detailed in Section S5 of the Supporting Information, the label authenticates even after 124 h of such exposure. A good photostability of the inorganic phosphors is unsurprising, given these are developed for color conversion in, e.g., LEDs wherein they experience a prolonged high light intensity and heat.

Furthermore, by moving to the fully PDMS design, the labels become flexible. This means that they can be conformally applied to a curved surface. An example of this is shown in S6 of the Supporting Information, with the PDMS label applied to the curved surface of a bottle, and a demonstration of the different patterns observed as the bottle is rotated with respect to the smartphone. This ability to conformally coat is advantageous, but we must mention that the label must be held with the same curvature for the testing in the field as it was for the initial reference characterization. That is, if the label was held flat for the reference image creation, it must also be held flat for the test image generation.

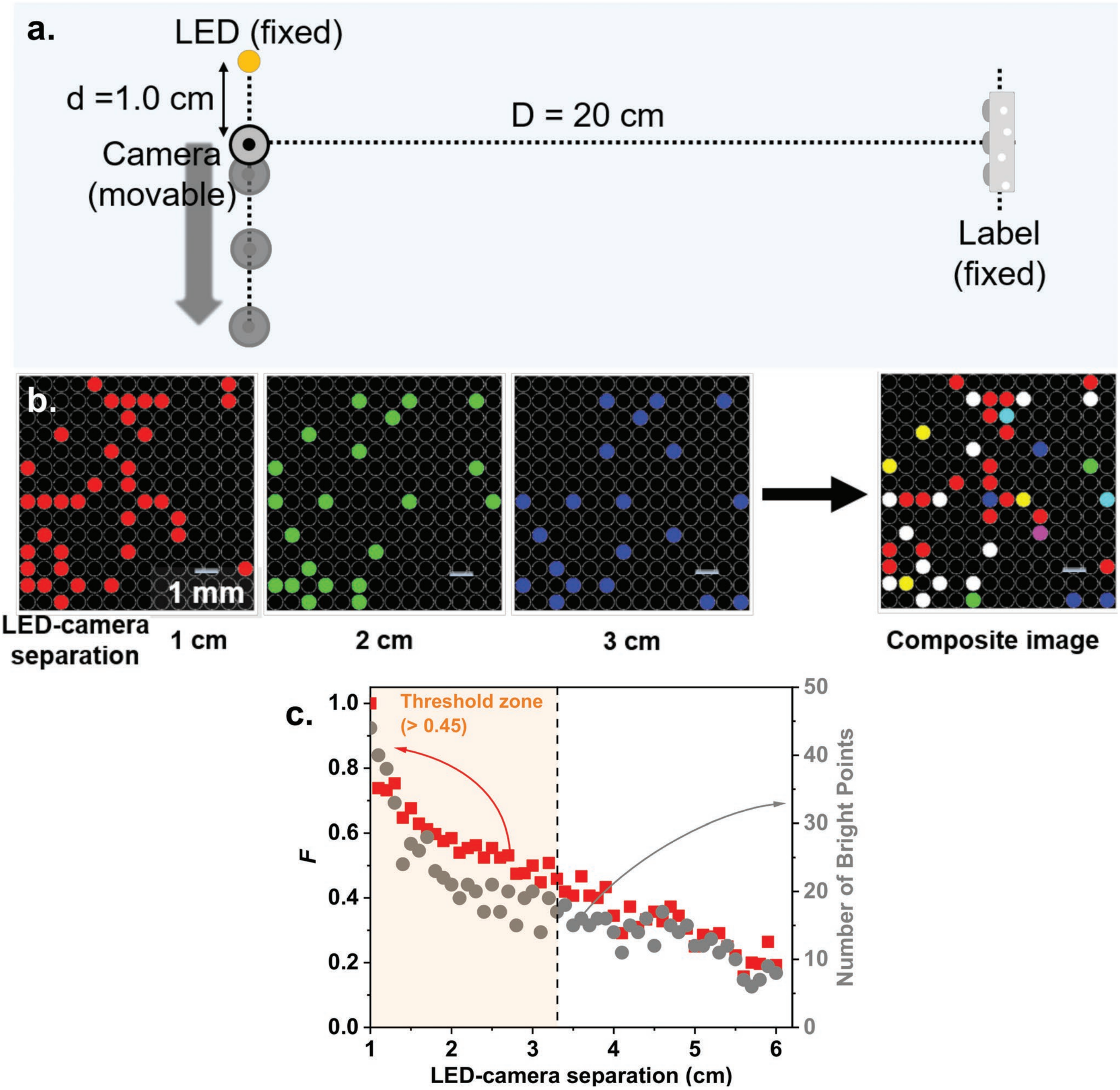

Figure 6. a) Schematic of setup for varying the LED–camera distance. b) Comparison of bright point patterns obtained with LED–camera distances of 1, 2, and 3 cm. c) Fraction of bright points in the same locations, *F*, for comparison of test image at indicated LED–camera separation with the reference image at separation of 1.0 cm. Also, the number of bright points in the test image at the given separation.

3. Conclusions

We have demonstrated that unclonable anticounterfeiting labels based on a microlens array and a microphosphor-loaded polymer layer can be authenticated with a single smartphone. We translate the bright point pattern underneath the 14 × 14 lens array to a 196bit binary string that represents the microlenses that led to a bright emission point. Such strings generated from the reference and test images allow very fast classification of whether or not the test and reference images match (and therefore authenticate). We find that, if the smartphone is repositioned to a tolerance of less than 1 cm for the capture of the test image, then the test image will authenticate with the reference. This tolerance is consistent with simple hardware for establishing the relative position of the smartphone and label in the field. We also note that the extremely low computational cost and high speed of comparing a single test image with multiple reference images could be used to further widen this tolerance by comparing a single test image to a few different reference images taken over a range of positions. We also establish that the authentication is not precluded by variation of the LED–camera separation, as long as this separation is

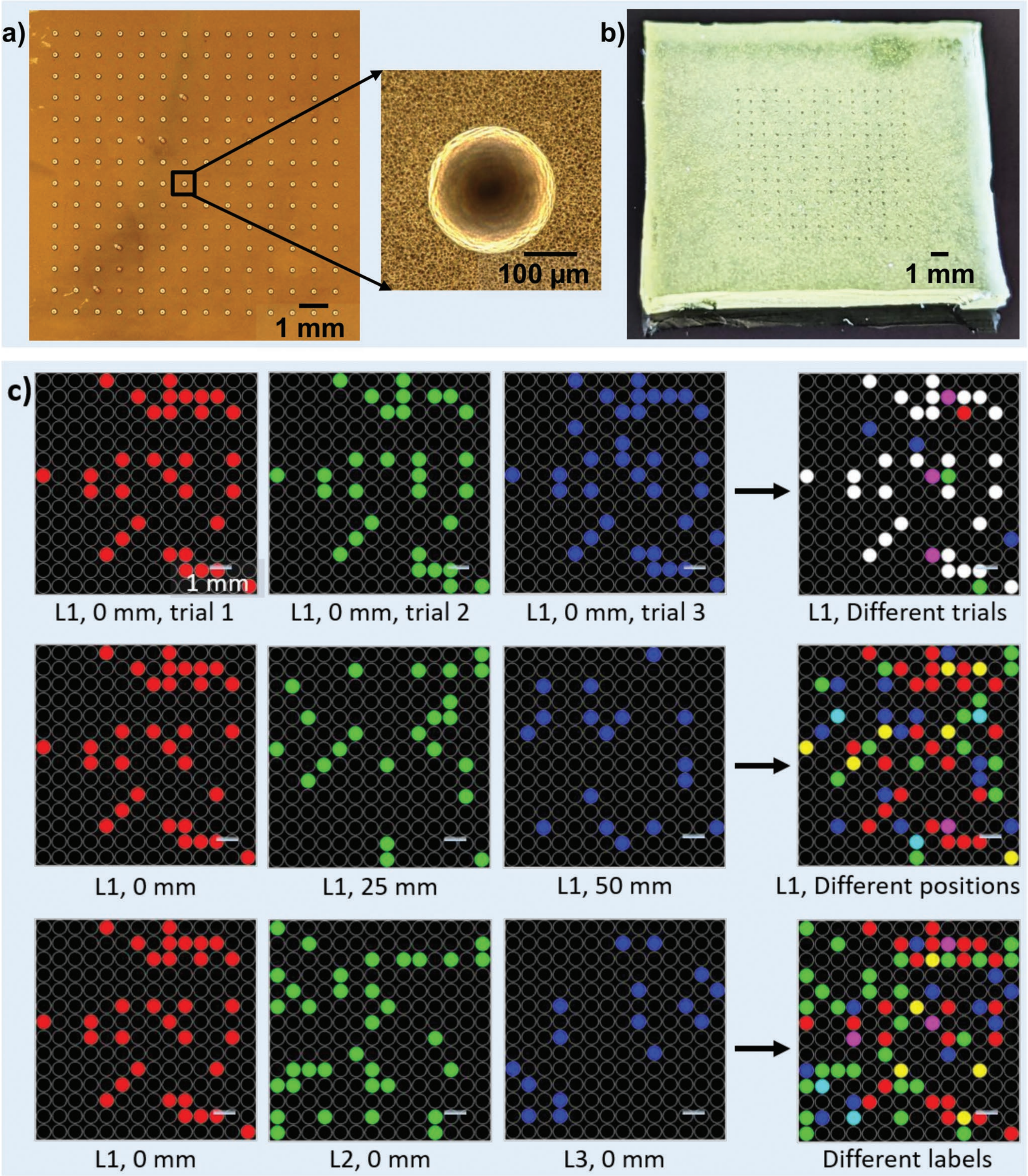

Figure 7. a) Image of negative structure replicated on nickel shim. Single-layer PDMS labels are created by pouring microphosphor-loaded PDMS onto this master. b) Photograph of the single-layer PDMS labels. c) Qualitative analysis of PDMS single-layer labels (in analogy with Figure 3) to demonstrate that they perform in the same way as the PDMS–glass labels.

less than 3 cm. The requirement of an LED–camera separation of less than 3 cm is met by all smartphones we are aware of. In summary, this is a significant step forward toward realizing an unclonable label that can be authenticated using a single smartphone. To reach the ultimate target of allowing authentication by a handheld smartphone without any additional components, we will concentrate future work on removing the need for the optical filters (potentially employing scattering rather than luminescence), and also on developing algorithms for on-the-fly determination of the phone position relative to the label and appropriate classification. Such developments would increase the practical utility of this label design, while maintaining the advantage in terms of security that this approach has over its competitors in the variation of the bright point pattern with smartphone position.

4. Statistical Analysis

The population size (number of labels and/or images) is mentioned in each figure, and the statistical analysis presented in Figure 4 is used to estimate the probability of authentication. The full algorithms to generate the figures and the acquired images to input into these are available at the source mentioned in the Data Availability Statement Section.

Supporting Information

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

Acknowledgements

The authors thank the Helmholtz Association for support through: 1) the Helmholtz Materials Energy Foundry (HEMF); 2) a recruitment initiative fellowship for B.S.R.; 3) KNMFi, and 4) MTET program (Materials and Technologies for the Energy Transition) —Topic 1—Photovoltaics (38.01.05). V.K. expresses gratitude to the DAAD for financial support. The authors acknowledge Dr. Markus Guttmann and Dr. Arndt Last at the Institute of Microstructure Technology (IMT) at KIT for their technical support provided during the label development and characterization.

Open access funding enabled and organized by Projekt DEAL.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability Statement

The data that support the findings of this study are openly available in Gitlab repository at https://git.scc.kit.edu/zl3429/label-authentication-algorithm-for-smartphone-application, reference number 34775.

Keywords

anticounterfeiting, microlens array, smartphone authentication

Received: August 9, 2022
Revised: October 26, 2022
Published online:

[1] a) P. Stryszowski, M. Kazimierczak, N. Wajsman, P. Avery, OECD/EUIPO, *Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risk, Illicit Trade*, OECD Publishing, Paris **2022**; b) R. Handfield, Counterfeiting is on the Rise and Projected to Exceed USD 3 Trillion in 2022, https://scm.ncsu.edu/scm-articles/article/counterfeiting-is-on-the-rise-projected-to-exceed-3-trillion-in-2022 (accessed: August 2022).

[2] L. Lynott, C. Dujovski, D. O'Connor, Fighting Respirator Fraud Globally Every day, https://multimedia.3m.com/mws/media/1862180O/3m-covid-19-infographic-print-version.pdf (accessed: August 2022).

[3] a) R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*, Springer, Berlin, Heidelberg **2013**; b) R. Arppe, T. J. Sørensen, *Nat. Rev. Chem.* **2017**, *1*, 0031; c) Y. Gao, S. F. Al-Sarawi, D. Abbott, *Nat. Electron.* **2020**, *3*, 81.

[4] a) Y. Gu, C. He, Y. Zhang, L. Lin, B. D. Thackray, J. Ye, *Nat. Commun.* **2020**, *11*, 516; b) M. R. Carro-Temboury, R. Arppe, T. Vosch, T. J. Sørensen, *Sci. Adv.* **2018**, *4*, e1701384.

[5] a) R. Arppe-Tabbara, M. Tabbara, T. J. Sørensen, *ACS Appl. Mater. Interfaces* **2019**, *11*, 6475; b) A. Fernández-Benito, M. Hoyos, M. A. López-Manchado, T. J. Sørensen, *ACS Appl. Nano Mater.* **2022**, *5*, 13752; c) B.-H. Wu, C. Zhang, N. Zheng, L.-W. Wu, Z.-K. Xu, L.-S. Wan, *ACS Appl. Polym. Mater.* **2018**, *1*, 47.

[6] V. Kumar, S. Dottermusch, N. Katumo, A. Chauhan, B. S. Richards, I. A. Howard, *Adv. Opt. Mater.* **2022**, *10*, 2102402.

[7] V. Kumar, S. Dottermusch, A. Chauhan, B. S. Richards, I. A. Howard, *Adv. Photonics Res.* **2022**, *3*, 2100202.

[8] J. Wu, X. Liu, X. Liu, Z. Tang, Z. Huang, W. Lin, X. Lin, G. Yi, *Chem. Eng. J.* **2022**, *439*, 135601.

[9] Y. Liu, Y. Zheng, Y. Zhu, F. Ma, X. Zheng, K. Yang, X. Zheng, Z. Xu, S. Ju, Y. Zheng, *ACS Appl. Mater. Interfaces* **2020**, *12*, 39649.

[10] M. S. Kim, G. J. Lee, J. W. Leem, S. Choi, Y. L. Kim, Y. M. Song, *Nat. Commun.* **2022**, *13*, 247.

[11] N. Torun, I. Torun, M. Sakir, M. Kalay, M. S. Onses, *ACS Appl. Mater. Interfaces* **2021**, *13*, 11247.

[12] N. Kayaci, R. Ozdemir, M. Kalay, N. B. Kiremitler, H. Usta, M. S. Onses, *Adv. Funct. Mater.* **2022**, *32*, 2108675.

[13] A. Esidir, N. B. Kiremitler, M. Kalay, A. Basturk, M. S. Onses, *ACS Appl. Polym. Mater.* **2022**, *4*, 5952.

[14] C. Wang, Z. Yan, C. Gong, H. Xie, Z. Qiao, Z. Yuan, Y.-C. Chen, *ACS Appl. Mater. Interfaces* **2022**, *14*, 10927.

[15] D. J. Farrell, PVtrace, https://github.com/danieljfarrell/pvtrace (accessed: August 2022).