Heliyon 10 (2024) e22895

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Biocompatible optical physically unclonable function hydrogel microparticles for on-dose authentication

Mengmeng Zhang [a], Aparna Raghunath [a], An Zhao [a], Huseyin Burak Eral [a,b,*]

[a] Process & Energy Department, Delft University of Technology, Leeghwaterstraat 39, 2628 CB Delft, the Netherlands
[b] Van't Hoff Labs, Physical Chemistry, University of Utrecht, the Netherlands

ARTICLE INFO

Keywords:
Anti-counterfeiting
On-dose authentication
Physical unclonable function
Biocompatible
Hydrogel
Colloid
Emulsion
Optical PUF

ABSTRACT

On-dose authentication (ODA) enhances security by incorporating customized molecular or micro-tags into each pill, preventing counterfeit products in genuine packages. ODA's security relies on tag non-replication and non-reverse engineering. Combining ODA with graphical Physical Unclonable Functions (PUF) promises maximum security. PUF uses intrinsic micro or nanoscale randomness as a unique 'fingerprint'. However, current graphical PUFs have limitations like specific illumination requirements and the use of toxic materials, restricting their use in pharmaceuticals.

In this study, we propose a novel approach called on-dose PUF. This method involves embedding microspheres randomly within micro biocompatible hydrogel particles. We showcase two distinct types of such on-dose PUFs. The first type utilizes randomly distributed superparamagnetic colloids (SPC) of identical diameters, while the second type utilizes vortexed sunflower oil drops of various diameters. The diameter and coordinates of the microspheres serve as input for generating cryptographic keys. A universal circle identification and binning program is used for extracting this information. One advantage of this approach is that it enables imaging using white light illumination and low-magnification microscopy, as color and signal intensity information are not crucial. This method enables patients to verify their medication by using their mobile phones from home.

To assess the performance of the proposed on-dose PUF, we conducted canonical investigations on the single-diameter system. This system can only generate one layer of cryptographic keys, making it potentially more vulnerable than the multiple-diameter system. However, the single-diameter system successfully passed NIST Statistical tests and exhibited sufficient randomness, ideal bit uniformity, Hamming distance, and device uniqueness. Furthermore, we found that the encoding capacity of the single-diameter system was 9.2×10^{18}, providing ample labeling potential.

1. Introduction

Counterfeit food and pharmaceuticals are a global threat with dire consequences to the health of millions worldwide [1]. The already existing measures such as barcodes, QR codes, and serial numbers on the packaging do not alleviate the problem as they

* Corresponding author.
E-mail address: h.b.eral@tudelft.nl (H.B. Eral).

https://doi.org/10.1016/j.heliyon.2023.e22895
Received 5 September 2023; Received in revised form 20 November 2023; Accepted 22 November 2023

Available online 5 December 2023

can be easily reproduced by counterfeiters. More than that, elaborate packaging would cause the overuse of plastics and exacerbate environmental issues.

To combat rampant counterfeiting on packaging, on-dose authentication (ODA) tags were introduced. ODA tags are usually biocompatible and directly embedded into the end products themselves to enable verification of their origin and safety even in the absence of packaging. A few prototypes of ODA tags, from microtaggants [2–6] to macro films [7,8] including various on-dose printing technologies [9–11] have been demonstrated in recent years. ODA tags are a more robust, resilient, and environmentally friendly alternative to traditional authentication protocols, as they are integrated into solid drugs rather than relying on packaging [12]. However, ODA tags may not yet be at the highest level of safety. For instance, barcodes produced by flow lithography [3,5] are susceptible to cracking and cloning by sophisticated criminals who have access to the same techniques. In this case, a combination with Physical Unclonable Functions (PUF), i.e., an on-dose PUF that creates an authentication system that cannot be duplicated, is considered an effective solution [7].

Originally developed for hardware and information security, PUF has been an important component for highly secure anti-counterfeiting systems since it was first introduced by Pappu et al. [13]. PUFs come in varied forms [14], including silicon-based PUFs, ring Oscillator PUFs, SRAM PUFs, biometric PUFs, and optical PUFs. Each type of PUF employs specific mechanisms to produce distinct identifiers. Recently, optical PUF was successfully translated by Leem et al. [7] for tagging pharmaceuticals. To avoid any confusion, the term PUF in this study only refers to physical optical tags for authentication that utilize intrinsic randomness at the microscale or nanoscale introduced during fabrication processes as a unique 'fingerprint' [15].

PUF is usually described as a black box [16] through which input challenges are passed and output responses are returned. It is almost impossible to generate two identical output responses because the PUF tags are fabricated via chemical methods in a stochastic process. By raising the system entropy, the randomness of the resulting PUF tags is immensely increased and consequently ensures the uniqueness of each tag. In this way, it is easy to create but extremely difficult or expensive to clone a particular PUF tag, even using the manufacturer's methods [16]. Since responses are unpredictable, the authentication is secured.

If we view the PUF tag as a type of physical lock, the encoding process, which involves generating a response based on an input challenge, can be thought of as creating a key. It usually involves steps such as the acquisition and digitization of graphical patterns. Taking the example of the PUF system using fluorescent proteins for tagging pharmaceuticals as mentioned above [7], a fluorescence microscope is used under various excitation wavelengths (inputs) to get corresponding unique images (outputs). These images are further digitized into a corresponding cryptographic key, or a 'digital key', via a particular algorithm. This key is stored in a secure database prior to labeling. To authenticate, a key produced by a certain 'physical lock' is compared to the 'digital key' in the database. If two keys match, the labeled product can be considered genuine.

Moreover, a PUF can be created to have an exponential number of input challenge-output response pairs for high security. The end-users can retrieve all the information about the medicine such as the origin, expiry date, side effects, etc. from a database by using a particular reader which will produce the output after scanning the tag and matching it with the stored 'digital keys'.

The fabrication process, image acquisition, and digitization algorithm are crucial to avoid any false reading of on-dose PUF tags. On top of that, the materials adopted should be completely biocompatible. Efforts to prevent counterfeiting using on-dose PUF tags are still in the early stages of development, and there have been few published studies on the topic. Regrettably, the key factors mentioned above have not yet been fully met for practical application.

Material selection stands as the primary consideration. To date, PUF is reported to have been fabricated with carbon nanotubes [17], cholesteric liquid crystal [18], lanthanide (III) ion dopants [19], rare-earth upconversion nanocrystals [20], and long-lasting fluorescent nanoparticles called quantum dots [21]. Unfortunately, most of these ingredients are toxic and hence forbidden for pharmaceutical applications. Ensuring biocompatibility is crucial in on-dose authentication. Recently, colloidal metal nanoparticles [22–25] have been introduced as an alternative ingredient for on-dose PUF. While certain studies claim the bio-safety of the aforementioned materials, no direct biological toxicity assessments have been conducted specifically regarding PUF. Prior to on-field application, it is imperative to conduct toxicity testing. Esidir et al. [26] introduced a food-grade PUF based on fluorescent dye-embedded corn starch particles. However, another general problem that arises from fluorescent dyes is the short lifetime due to their easy quenching under improper storage [19]. In this case, the response tends to be unreliable, which can lead to incorrect determinations regarding authenticity. Lately, silk, acknowledged for its safety in general use (known as GRAS according to the FDA), has been favored by researchers in the field of on-dose authentication due to its biological safety and ease of genetic hybridization [7,27–29]. Additionally, biocompatible Polyethylene glycol diacrylate (PEGDA) [30] demonstrates promising potential [5,31]. We look forward to embracing more materials from the GRAS category in this application field, to circumvent the time-consuming and costly toxicological studies [32].

The selection of material further restrains the method of image capture. For instance, fluorescent PUF tags are specifically acquired via fluorescence microscopy while metal nanoparticles and liquid crystal PUF need to be observed under a dark field microscope, or a Raman microscope [24,27,33,34]. Specifically, Demirok et al. [35] presented a PUF system based on alloy nanowires that can be read in multiple manners including X-ray fluorescence spectrometer, electrochemical microscope, and magnetometer. These techniques were thought to enhance the overall security of the PUF system. However, such sophisticated and bulky appliances constrain the readout to advanced labs. As a result, the reading cost unavoidably increases tremendously when every pharmaceutical tablet needs to be labeled.

For practical applications, one needs to consider the image quality when extracting the patterns. External perturbation cannot always be avoided since pattern recognition is often conducted under different conditions. For instance, the conditions under which the image is obtained for recognition to store the 'digital key' in the database may not be similar to the 'authentication key' at the user's end. The presence of complex patterns in this case instead becomes a drawback in terms of the image quality.

To counter the dire need for high-fidelity images, image processing algorithms usually involve multiple steps such as background correction, color differentiation, binarization, intensity value normalization, etc. [36,37]. The final step of encoding is the recognition of the characteristic pattern via a certain algorithm. The algorithms in terms of this field vary and are decided by the patterns. Similar to fingerprint identification where the ridge information is often analyzed [19], the positions and colors of the particles are usually recorded pixel by pixel for particle-embedded PUFs [24,33]. When the characteristic pattern is composed of nanotubes or nanowires, the orientations or rotational degrees of these lines are often recorded [19,38]. In other words, color, position, and orientation are generally adopted as inputs.

The corresponding output information is further digitized to reduce the size of the stored data and subsequently reduce the time required for the authentication process [25]. It is worth noting that the input/output complexity positively correlates with the computational cost which we usually wish to minimize to the level that even a mobile phone is sufficient for the user.

Finally, we should consider the authentication algorithm. A widely used model to determine the similarity between two images is comparing them to each other [39]. Such operation is acceptable when dealing with small sets of images, but it will be very expensive computationally to individually compare each PUF since the database contains billions of 'digital keys'. For this reason, the string matching method is usually chosen but is still quite costly when the database is huge.

In conclusion, while the aforementioned PUFs are a noteworthy advancement in the realm of anti-counterfeiting, their practical applications are currently restricted due to limitations arising from material selection, image acquisition methodology, and encoding algorithms as discussed earlier.

In this study, we present two types of biocompatible PUF microparticles that utilize microsphere diameter and coordination as input. They are fabricated by embedding microspheres into a biocompatible matrix, Poly(ethylene glycol) diacrylate (PEGDA). The first design showcases a single-diameter on-dose PUF, where randomly distributed superparamagnetic colloids (SPCs) of identical diameters are embedded into PEGDA. The second design features a multiple-diameter system, achieved by embedding sunflower oil droplets of various diameters into PEGDA using a vortex-induced oil-in-water method. These microparticles, due to their biocompatibility and suitability for direct application at the dosage level, are referred to as on-dose PUFs. To extract information from the PUF microparticles, we propose a PUF working algorithm that only requires the diameters and coordinates of the spheres as input. A universal Matlab program capable of circle identification and binning is used to simplify the encoding process. As color and intensity are not utilized as inputs, image acquisition can be accomplished using common illumination and low-magnification microscopy. Furthermore, the performance of the single-diameter PUF was thoroughly examined using a sample size of 16 keys and evaluated using the NIST Statistical Suite (National Institute of Standards and Technology). The results demonstrate that the cryptographic responses exhibit sufficient randomness. Additionally, the single-diameter on-dose PUF exhibits an impressive encoding capacity of 9.2×10^{18}, capable of accommodating substantial labeling requirements.

2. Results and discussion

2.1. Two types of on-dose PUF microparticle

2.1.1. Single-diameter on-dose PUF

The first on-dose PUF microparticle employs single-diameter as input and its synthesis via stop-flow lithography is depicted in Fig. 1 (a). Firstly, a suspension containing UV-responsive oligomer PEGDA, a photoinitiator, and superparamagnetic colloids (SPCs) are pumped into the microchannel. After the channel is filled, flow is stopped, and an external magnetic field is imposed using a Halbach array magnet. SPCs align when the magnetic field is parallel to the platform and segregate homogeneously when the vertical magnetic field dominates, as shown in Fig. 1 (b). Homogeneous and stochastic distribution of SPCs is crucial, as it serves to eliminate the bias in encoding from the very beginning. Thereafter, UV light passes through a mask to trigger photo-polymerization, and the on-dose PUF in a particle shape can be obtained (see Fig. 1 (e and f)).

Now that the diameter functions as input, microspheres are expected to be fixed in the same depth in this hydrogel microparticle to prevent invalid readings. Without a doubt, the settlement facilitated by gravitational force and Brownian motion will also generate a random scattering of SPCs at the gel bottom. Nevertheless, here, the Halbach magnet accelerates the settling speed of the colloids so a faster fabrication can be achieved, a benefit magnetic trapping can bring. There are several other benefits of stop-flow lithography. For instance, the geometry of the final on-dose PUF microparticles can be independently controlled by a mask, consequently, the size of on-dose PUFs can be precisely manipulated on a micron scale. Furthermore, images of each microparticle can be recorded simultaneously by the microscope and saved for further processing, which can boost the efficiency of digital key generation. In this manner, database registration can be achieved without slowing the production line. This assists in minimizing the additional cost incurred for the product. Together, these characteristics endow higher security of our microparticle as well as keep the cost at an affordable level.

In addition to the previous discussion, there might be concerns about the biosafety and cytotoxicity of this microparticle. The same ingredients have already been adopted by our group previously in an on-dose microparticle and their biosafety has been thoroughly discussed [5]. PEGDA, iron oxide nanoparticles, and polystyrene trace within SPC (daily intake <1.5 mg [40]) are considered biocompatible and approved for clinical applications due to their acceptable biosafety, supporting various pharmaceutical formulations. Furthermore, this single-diameter type can be easily applied using other biocompatible microspheres, such as synthetic polymeric microspheres, which are widely used in medical applications [41].

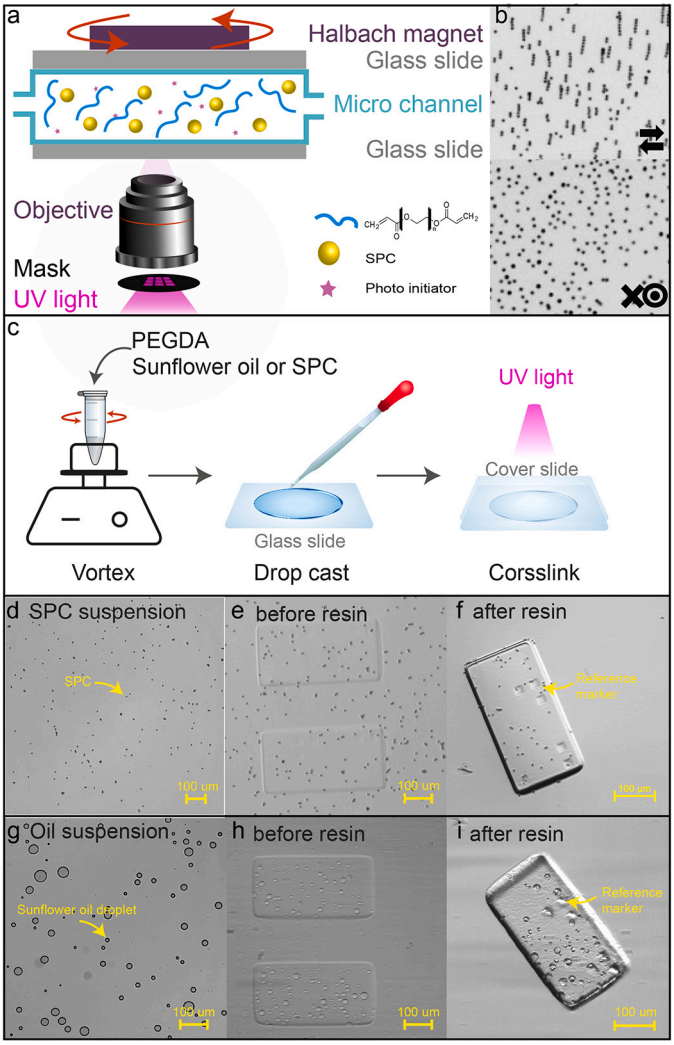

Fig. 1. Two types of on-dose PUF design: The single-diameter type is created by employing stop-flow lithography of superparamagnetic colloids (SPCs) within Poly(ethylene glycol) diacrylate (PEGDA) (a). The alignment of SPCs is controlled using oriented magnetic fields, as demonstrated in (b). Initially, a suspension of homogeneously and stochastically distributed SPCs is obtained (d), followed by photosynthesis into microparticles. The images of the single-diameter microparticles before and after resin are shown in (e) and (f) respectively. On the other hand, the multiple-diameter type is produced through vortex and drop-casting of sunflower oil and PEGDA suspension, as depicted in (c). The homogeneous and stochastic distribution of oil droplets is first achieved as a suspension (g) and then transformed into microparticles via photosynthesis. The images of the multiple-diameter microparticles before and after resin are presented in (h) and (i) respectively. An array of hollow squares collectively serves as a reference marker to mitigate the impact of rotation or other potential variations during the authentication process.

2.1.2. Multiple-diameter on-dose PUF

A multiple-diameter on-dose PUF was prepared via drop casting of immiscible oil/water phase suspension as shown in Fig. 1 (c). Here, sunflower oil was used as the oil phase while PEG700 was used as the water phase. Followed by a short vortex, the suspension was drop cast and cross-linked by UV light. After peeling from the substrate, a glass slide in this study, a suspension containing various oil droplets is ready as seen in Fig. 1 (g). Moreover, this suspension can also be fabricated into particles if a mask is adopted as shown in Fig. 1 (h and i).

When two immiscible substances are mixed, the disperse phase will form a spherical shape due to the surface tension. This phenomenon is widely seen in daily life such as the oil droplets in broth. With no control, the dispersed phase tends to create droplets over a wide size distribution, a major factor governing the generation of the PUF pattern, being desirable for multiple inputs. As showcased in Fig. 1 (g), the locations at which those droplets form and their diameters are stochastic parameters. The randomly distributed droplets of various sizes jointly represent the fingerprint patterns. Moreover, the interface between oil and water is distinct for clear visualization due to their appreciable difference in refractive index. Therefore, the droplets can be observed under common illumination sources including sunlight. It is worth noting that there are various ways to create such a wide size distribution, including but not limited to sonication, homogenization, and microfluidic drop-wise emulsification [42], as well as the vortex as showcased in this work. In addition, advanced microspheres such as multi-compartmental microspheres fabricated by gas-shearing [40,43], microspheres with protrusions and cavities in various shapes [44] can also be transplanted to this system to further

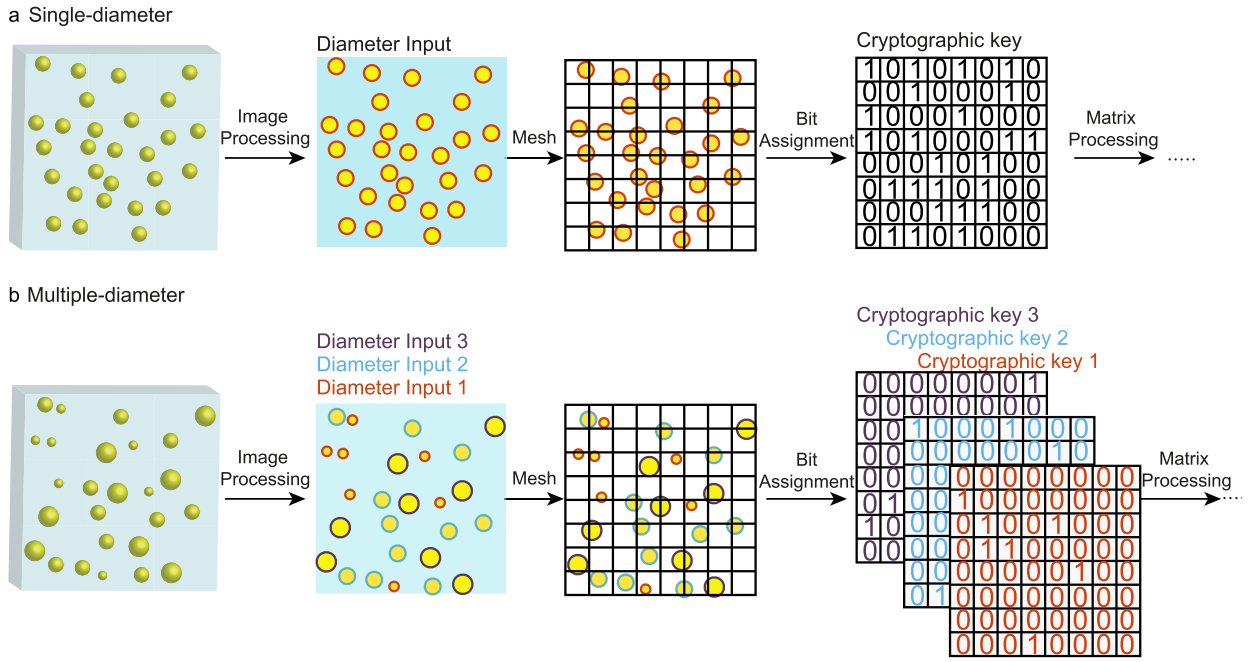

Fig. 2. Schematic illustration of working algorithm. Cryptographic keys are generated from a diameter-based PUF authentication system using (a) single diameter and (b) multiple diameters as input. Following proper mesh and bit assignment, the cryptographic key, i.e. the output response matrix is further processed depending on the bit uniformity.

improve the safety level by extremely boosting the complexity of patterns. Similarly, the concept of generating unique patterns by randomness is not limited to the materials shown in this work and should be readily applicable to other types of materials.

In summary, the proposed on-dose PUF that utilizes microsphere diameter and coordination as input showcases versatility. It can be fabricated using different methods and ingredients. In the subsequent section, we will present a universal program designed to extract information from these PUFs.

2.2. *Working algorithm*

Fig. 2 (a) and (b) schematically illustrate the working protocols of key generation using the single diameter and multiple diameters as input respectively. After a proper image of the PUF tag is captured and meshed per certain amounts of pixels, it is processed in Matlab using earlier developed algorithms Hough transform [45]. Via the 3 steps in the Hough transform, i.e., greylization, binarization, and circle detection, the pixel coordinates for the centers of the spheres of a certain diameter input are extracted. After the spheres are identified, the coordinates of the center are then used to make a binary matrix the same size as the mesh. Cells in the binary matrix get assigned a value of *1* when the corresponding pixel in the image contains the center of a sphere, and *0* otherwise. Hough transform is widely used as it saves time using no loops to get a fast circle detection. The 3 steps of the Hough transform are summarized in Supplementary Table S1 and showcased in Supplementary Figure S1. The MatLab code can also be found in Supplementary 4.3. We recognize the low-contrast optical images as showcased in Fig. 1 (d-i) can challenge image processing. To address this, we can employ various contrast-enhancement techniques like histogram equalization [46] and local adaptive contrast enhancement [47]. Additionally, methods such as Otsu's adaptive thresholding [48] can enhance the reliability of the binarization process. We acknowledge the potential benefits of such techniques and their relevance in more refined applications, they may be beyond the scope of our current study.

Since the parameter of diameter can be arbitrarily chosen in the Hough transform, we can manipulate the number of inputs. For instance, for a single-diameter PUF with 5 μm spheres, a binary matrix will be returned if 5 μm is input. However, no circles will be detected if other diameters are input so a zero matrix will be returned instead. In this way, only the correct diameter can yield the desired response. We will not worry if the diameter is known by counterfeiter because the distribution of bit 1 is random so each response is unique, which will be demonstrated in the following section.

Stronger security can be achieved by a multiple-diameter PUF with spheres of various sizes as shown in Fig. 2 (b). We can enter different inputs, and each input will return a corresponding output. In this way, several layers of cryptographic keys are generated. If the diameters of the spheres, or say, the adopted inputs for key generation, are unknown, the attacker cannot enumerate all possible inputs in a short time. If known, the PUF pattern from a PUF tag with 3 different circle sizes has 4 possible responses at each mesh point. This large challenge–response space makes the prediction almost impossible thanks to the exponential response produced. Still, readout time should be taken into consideration jointly with the input number to obstruct the total enumeration of the PUF [16].

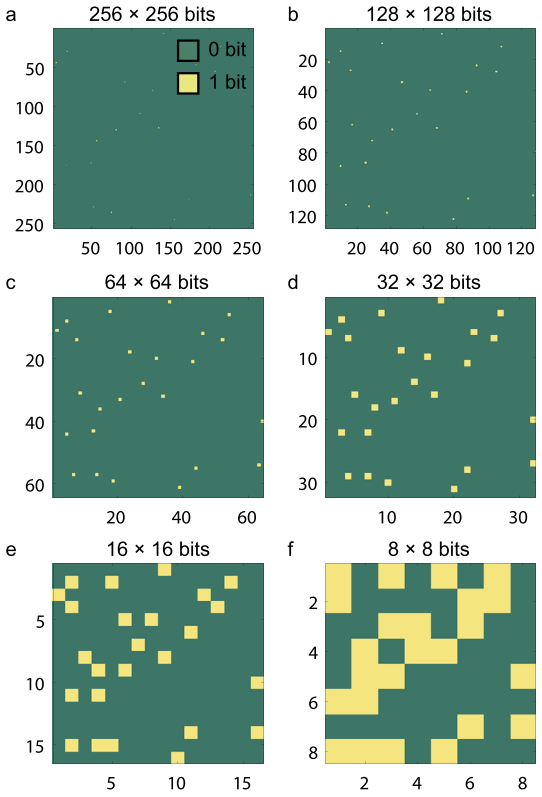

Fig. 3. Data binning of the output response matrix. An original matrix of 512×512 is scaled down to (a) 256×256 in the first binning, and then to (b) 128×128, (c) 64×64, (d) 32×32, (e) 16×16 and finally to (f) 8×8. At this point, it is apparent that the proportion of *0*s and *1*s is closer to 0.5.

After the matrix is assigned, a bias might show up. We can observe a significant bias toward the "*1*" state if the concentration of materials that loaded to produce circles is too high, or a bias to "*0*" when the concentration is too low. If we take the example of a 512×512 pixel Physical Unclonable Function (PUF), which contains approximately 28 spheres as illustrated in Fig. 3 (Response Binned ×1), it implies that on average, only 28 cells out of the total 512×512 cells in the matrix hold the value of *1*. This indicates a significant bias towards *0* in the data, meaning that it is more probable for a cell to contain a *0* than a *1*. Therefore, such data is more susceptible to key prediction attacks, and it is favorable to reduce the amount of *0*s in this case.

There are various algorithms to reduce entropy leakage such as by utilizing a corrector. In this study, the response matrix was scaled down from 512×512 to 8×8 by applying data binning 6 times with a special rule applied to create the bins. The special rule is that the highest number in the bin is chosen to represent the bin. Since the matrix only contains the logical values of *0* and *1*, any bin containing even a single instance of the value of *1* will be represented by *1*. This binning will reduce the instances of *0* appearing in the matrix thus making it more secure by decreasing bias in the final digital key while retaining the spatial arrangement of the spheres in the physical key. In this way, the binning process is repeated to reach a final 8×8 size with a total of 64 cells. An example of the binning process is presented in Fig. 3. It can be seen how the distribution of *1*s in the initial matrix develops with each time the binning process is applied. It is important to emphasize that this particular rule applies exclusively to the dataset at hand, characterized by the presence of 28 zeros within a 512×512 matrix. Further insights into the effectiveness of this binning approach will be presented in Section 2.3. Thereafter, these response matrices can be stored in a secured database for comparison with the 'authentication key'.

The CPU time and wall-clock time of this circle finding and binning of images in 2048 × 2048 pixels are measured on a laptop (3.0 GHz, Dell Latitude 7320, Quad-Core) using Matlab Online version. The average CPU time was 4.7 seconds while the average wall-clock time was 2.5 seconds. If we implement this set of codes on mainstream mobile phones that are at least equipped with a 2.4 GHz CPU, the wall-clock time would be about 3.2 seconds, which is expected to be within users' acceptance considering the scanning time of QR code in 2953 bytes is reported to be up to 0.5 seconds [49].

Overall, such a working algorithm of key generation using diameter as inputs combined with matrix binning avoids any expensive imaging system and is computationally efficient. The utilization of an affordable magnification hooked to a mobile phone to capture images of microtags has been successfully showcased by Rehor et al. [31]. Thus reading a PUF via mobile phone by general users is possible. Moreover, our algorithm removes the hindrance of synthesizing biocompatible PUF tags, now that toxic fluorescence ingredients are unnecessary. However, a concern might arise that counterfeiters might have the potential to replicate and manipulate spatial patterns when given access to the tags. It's important to note that the foremost consideration for counterfeiters would be the cost associated with counterfeiting. In the field of authentication, the application of PUF does not guarantee absolute non-replicability

Table 1
The results of the NIST test: The P-value that resulted from each test is compared with the significance level (α of 0.01 in the first level test and 0.0001 in the second level test) to come to the conclusion of whether to accept the null hypothesis that the data is random.

Type of Test	Pass Rate	P-Value	Conclusion
Frequency Test (Monobit)	32/32	0.000954	Random
Frequency Test within a Block	31/32	0.299251	Random
Cumulative Sums (Forward) Test	32/32	0.739918	Random
Cumulative Sums (Reverse) Test	31/32	0.350485	Random
Run Test	32/32	0.178278	Random
Serial test	31/32	0.602458, 0.028181	Random
Approximate Entropy Test	31/32	0.178278	Random

Note: For a sample size of 32 binary sequences, the minimum passing rate for each statistical test is approximately 29.

but significantly incurs high replication costs, encompassing both time and financial investment. Moreover, we advise access control, such as restricting the number of authentications [50], to deter counterfeiters from extensively reproducing the same PUF label. This practice would add an additional layer of security against mass replication.

2.3. Evaluation of single-diameter on-dose PUF

2.3.1. Randomness test

A group of 16 single-diameter on-dose PUFs is produced and processed into 16 corresponding 'digital keys'. National Institute of Standards and Technology statistical test suite NIST SP 800–22 is adopted to assess whether any patterns can be detected that make it possible to predict the bit sequence. The results are summarized in Table 1. Here we canonically choose the single-diameter on-dose PUFs because it represents a single input and thus is more vulnerable to attack. The resulting 16 images are 512×512 pixels in size with 0.32 μm per pixel and are provided in Supplementary Figure S2.

SP 800–22 is a widely used package to test for randomness for Random Number Generator (RNG)s [51]. Statistical testing involved choosing a null hypothesis (H_o) and an alternative hypothesis (H_a). For the randomness test, they are *Data is random* for H_o and *Data is not random* for H_a respectively. NIST SP 800-22 includes a set of 15 one-level tests and 2 two-level tests, which assess various aspects of randomness. Each one-level test produces one or more p-values and returns as a pass rate (i.e., the proportion of the passed sequences), while the two-level tests evaluate the consistency of the p-values obtained from a particular one-level test.

To assess the validity of the null hypothesis and accept the alternative hypothesis, a significance level, denoted by α, is established for the P-value [51]. When $p \leq \alpha$, the null hypothesis is rejected, and the alternative hypothesis is accepted. To demonstrate that the data is random and the bits are uncorrelated with each other, higher P-values than α are preferred [52]. The significance level is dependent on the sample size, and the minimum sample size for a specific α can be calculated using mathematical computations [52]. For the first level of testing, the α value is set to 0.01, whereas for the second level, it is set to 0.0001, as per the NIST guidelines [53].

The investigation of each test in the group of 15 requires a minimum sequence length of the bitstream under investigation. In this study, the bitstream being tested is the combination of the digital keys of all 16 on-dose PUFs, resulting in a total sample size of 1024 as shown in Figure S3. The raw data are presented in Supplementary 4.3 and the summary of the NIST randomness tests' characteristics and the parameter values employed in each test can be found in Supplementary S2. Due to the short key size, only the tests that require a sequence length of less than 1024 are considered. Therefore, the selected tests for this study are the Frequency (Monobit) Test, Frequency Test within a Block, Runs Test, Longest Run of Ones in a Block, Serial Test, Approximate Entropy Test, and Cumulative Sums Test.

In Table 1, it can be seen that the bit stream from the digital key produced a p-value of a chi-squared ($\chi 2$) test and a pass rate in every test it was subjected to. The P-values are above the α. This means that the null hypothesis can be accepted for each test. Hence, the output from the on-dose PUFs is statistically random and consequently unpredictable, and thus unclonable.

2.3.2. Bit uniformity

Bit uniformity of the above 16 single-diameter PUFs is investigated and shown in Fig. 4 (a). Bit uniformity is the proportion of *1* bits in the bit sequence, which is also known as the Hamming Weight [7]. The distribution of Hamming Weights in the on-dose PUF system should be similar to a normal distribution. From Fig. 4 (a), the mean (μ) can be observed to be close to 0.5 which is the ideal value indicating only a low bias in the data. This indicator can be optimized by manipulating the binning times in this study as we have previously shown in Fig. 3. However, the binning will reduce the matrix size and consequently decrease the encoding capacity. This is not ideal when information-rich-PUF is needed. To avoid any unnecessary information loss, the concentration of the loaded SPCs is recommended to be precisely calculated before binning is applied. Furthermore, these 16 devices are obtained under the same equipment but with slightly different exposure, focus, contrast, and resolution. Their intra-chip hamming distance is shown in Supplementary Figure S5. With a mean intra-chip hamming distance of 3.589×10^{-3}, In addition to that, when considering a cut-off threshold of 0.0896, the derived false positive rate stands at 1.038×10^{-10}, while the false negative rate aligns at 0.

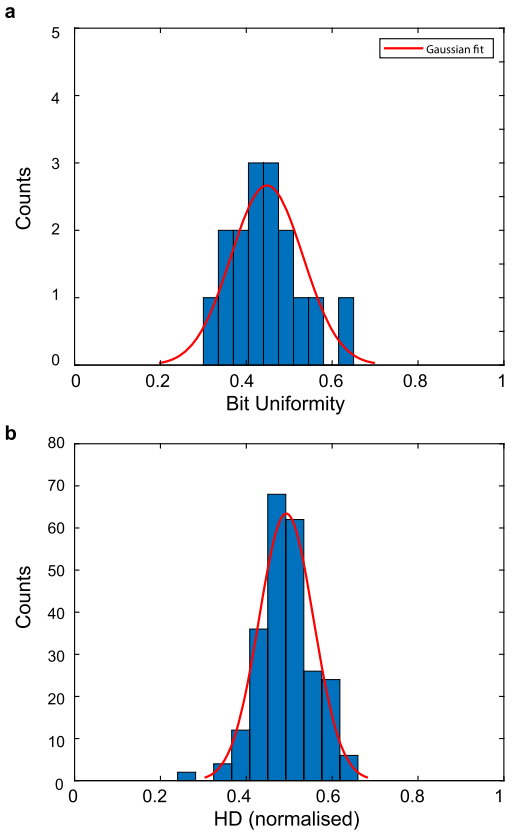

Fig. 4. Performance characteristics in bit uniformity and Hamming distance. (a) The bit uniformity of the 16 different digitized on-dose PUF keys shows a close resemblance to a normal distribution and the Gaussian fit of the data produces a mean (μ) of 0.45 with a standard deviation (σ) of 0.084. (b) The pairwise Hamming distances of the 16 different digitized on-dose PUF keys show a close resemblance to a normal distribution and the Gaussian fit of the data produces a mean (μ) of 0.49 with a standard deviation (σ) of 0.063. The pairwise Hamming distance can be found in Supplementary Figure S4.

2.3.3. Encoding capacity

At the same time, Hamming Distances were found for every pair of keys and shown in Fig. 4 (b). The Hamming Distance is the number of bits that differ at the corresponding positions in two PUF keys. C_{16}^{2} combinations are possible yielding 120 values which should also resemble a normal distribution when plotted (seen Supplementary S4). From Fig. 4 (b), the Gaussian fit of the Hamming Distance produces a μ of 0.49 and σ of 0.063 for this particular set of 16 PUFs. Since the Hamming distance is influenced by the similarities and differences between the keys, the μ and σ of the Gaussian fit can be used to find out the degrees of freedom of the PUF system by Equation (1). Using the degrees of freedom, the actual encoding capacity for this set of PUFs can be determined by Equation (2).

$$\text{Degrees of Freedom} = \frac{\mu \times (1-\mu)}{\sigma^2} = \frac{0.49 \times (1-0.49)}{0.063^2} \approx 63 \tag{1}$$

$$\text{Encoding Capacity} = 2^{63} = 9.2 \times 10^{18} \tag{2}$$

The Hamming distance distribution for this particular set of 16 PUFs is close to the ideal value of 0.5. With a single diameter input and a small encoding matrix of 8×8 cells, the encoding capacity already approaches 9.2×10^{18} for this conical case. This capacity will grow exponentially with the number of inputs. It is quite promising to reach the ideal encoding capacity of PUF which is approximately 10^{300} [19].

2.3.4. Device uniqueness

Finally, the probability of similarity in corresponding bits in two random PUF keys in the system, termed as the device uniqueness, is evaluated. There are several traditional uniqueness metrics available to evaluate the device uniqueness, here we choose the mean of the inter-device Hamming distance, i.e., HD_{mean} [7]. The outcome of HD_{mean} ranges from 0.0 to 0.5. The worst inter-device uniqueness is 0.0 when all devices generate the same signature. With a growing number of devices, this value can converge to 0.5, the most ideal value for uniqueness metric [54].

In this study, the HD_{mean} of the PUF system with mere 16 individual keys being investigated is calculated as 0.49, which is very close to the ideal value of 0.5. Thus, each key is considered as producing a unique response based on the entropy of the settling spheres.

3. Conclusion

On-dose PUFs have emerged as an appealing solution to tackle the rampant problem of counterfeit food and pharmaceuticals, due to the level of security and affordability they offer. In an effort to expand the possibilities of input methods, we propose a PUF working algorithm that leverages both the size of embedded objects (colloids and emulsion droplets) in a hydrogel particle and their coordinates as inputs. This study is the first exploration of its kind to utilize these parameters in optical PUFs to the best of our knowledge. Building on this idea, we developed two biocompatible on-dose PUF systems that rely on the entropy of randomly distributed SPCs or oil droplets to demonstrate the use of single or multiple inputs. The randomness and performance of the single-diameter PUF were evaluated and found to be ideal. These PUF microparticles can be read with bright field illumination. Moreover, the algorithm is computationally efficient, allowing for easy authenticity verification by general consumers, thus creating a significant hindrance to counterfeiting activities.

4. Experimental setup

4.1. Materials

Poly(ethylene glycol) diacrylate (average Mn 700), 2-Hydroxy-2-methylpropiophenone (CAS No. 7473-98-5) were purchased from Sigma-Aldrich. Silicon film of thickness 20 μm for the fabrication of microchannel was obtained from MyTech Ltd. The superparamagnetic microsphere PS-MAG-FluoYellow-COOH-AR488 with a saturation magnetization ranging from $15 \sim 25\ Am^2/\mathrm{kg}$, a density of 1.49 $\mathrm{g/cm^3}$ and a diameter of 4.54 μm was purchased from microParticles GmbH. The microsphere consists of a core made of polystyrene with iron oxide particles incorporated inside the polystyrene. The core is covered by a carboxyl group polymer shell with a thickness of 100-500 nm to prevent any leakage of the iron oxide particles to the surrounding medium. The SPCs are originally packaged as aqueous solutions containing 1wt% of particles that have a coefficient of variation of 5%. The sunflower oil is pursued from local supermarkets and used without any pre-processing.

4.2. Preparation of single-diameter PUF microparticle

A 2 cm × 1.5 cm silicon film was first cut. On it, a 1 cm × 1 cm square was hollowed out. The cut silicon film was then transferred to a glass slide. Two channels that connected the hollow area were carved to be used as an inlet and an outlet. After that, the ready channel was covered with a second glass slide and the microfluidic device was ready to use. The injected suspension is a mixture of photo-initiator (2-hydroxy-2-methylpropiophenone) with PEGDA-700 at a proportion 1:20 vol% and without any magnetic susceptibilities tuner to assure the edibility. To get a homogeneous distribution of the SPCs, the suspension was vortexed and placed in a sonication bath for 30 minutes at room temperature. The stop-flow lithography is conducted as previously described [5]. Their images were taken with the Andor CCD camera hooked up to the microscope (Nikon Ti-E inverted) at 20× magnification.

4.3. Preparation of oil/water PUF microparticle

A mixture of sunflower oil and PEG700 at a proportion 1:20 vol% was vortexed for 1 minute. 50 μL of the suspension was drop-cast to a glass slide and covered with another slide. After that, the liquid film was brought under UV light for 30 seconds and cured. Then the microparticle is finally ready. The liquid film was also cured under UV light through a mask to get PUF particles as stop-flow lithography.

Funding

This work is part of the research program open technology scheme with project number P80384, which is financed by the Dutch Research Council (NWO). Mengmeng Zhang was supported by a scholarship granted by the China Scholarship Council (CSC, Grant No. 201808370175).

CRediT authorship contribution statement

Mengmeng Zhang: Writing – review & editing, Writing – original draft, Supervision, Investigation, Formal analysis, Data curation, Conceptualization. **Aparna Raghunath:** Data curation. **An Zhao:** Data curation. **Huseyin Burak Eral:** Writing – review & editing, Writing – original draft, Supervision, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Mengmeng Zhang reports financial support was provided by China Scholarship Council. H.B. Eral reports financial support was provided by Dutch Research Council.

Data availability

Data included in article/supp. material/referenced in article.

Acknowledgements

We thank Dr. E. Mendes in the Chemical Engineering Department and Dr. R.M. Hartkamp in the Process and Energy Department at the Delft University of Technology for critical reading of the manuscript and useful suggestions.

Appendix A. Supplementary material

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.heliyon.2023.e22895.

References

[1] Anmole S. Bolla, Ashwani R. Patel, Ronny Priefer, The silent development of counterfeit medications in developing countries–a systematic review of detection technologies, Int. J. Pharm. 587 (2020) 119702.
[2] Sangkwon Han, Hyung Jong Bae, Junhoi Kim, Sunghwan Shin, Sung-Eun Choi, Sung Hoon Lee, Sunghoon Kwon, Wook Park, Lithographically encoded polymer microtaggant using high-capacity and error-correctable qr code for anti-counterfeiting of drugs, Adv. Mater. 24 (44) (2012) 5924–5929, https://doi.org/10.1002/adma.201201486, https://onlinelibrary.wiley.com/doi/abs/10.1002/adma.201201486.
[3] Ivan Rehor, Sophie van Vreeswijk, Tina Vermonden, Wim E. Hennink, Willem K. Kegel, Huseyin Burak Eral, Biodegradable microparticles for simultaneous detection of counterfeit and deteriorated edible products, Small 13 (39) (2017) 1701804, https://doi.org/10.1002/smll.201701804, https://onlinelibrary.wiley.com/doi/abs/10.1002/smll.201701804.
[4] Yug C. Saraswat, Fatma Ibis, Laura Rossi, Luigi Sasso, Huseyin Burak Eral, Paola Fanzio, Shape anisotropic colloidal particle fabrication using 2-photon polymerization, J. Colloid Interface Sci. 564 (2020) 43–51.
[5] Mengmeng Zhang, Thom Warth, Niels Boon, Ahmet Faik Demirörs, Hüseyin Burak Eral, Microfluidic synthesis of hydrogel microparticles with superparamagnetic colloids embedded at prescribed positions for anticounterfeiting applications, Adv. Mater. Interfaces (2022) 2200899.
[6] Toshiya Yasunaga, Takao Fukuoka, Akinobu Yamaguchi, Noriko Ogawa, Hiromitsu Yamamoto, Physical stability of stealth nanobeacon using surface-enhanced Raman scattering for anti-counterfeiting and monitoring medication adherence: deposition on various coating tablets, Int. J. Pharm. 624 (2022) 121980.
[7] Jung Woo Leem, Min Seok Kim, Seung Ho Choi, Seong-Ryul Kim, Seong-Wan Kim, Young Min Song, Robert J. Young, Young L. Kim, Edible unclonable functions, Nat. Commun. 11 (1) (2020), https://doi.org/10.1038/s41467-019-14066-5.
[8] Satoshi Takei, Safety-oriented photolithography of water-soluble resist using water-coating and water-developable processes for edible pharmaceutical polymer films, Appl. Phys. Express 11 (8) (2018), https://iopscience.iop.org/article/10.7567/APEX.11.086501.
[9] Krisztina Ludasi, Orsolya Jójárt-Laczkovich, Tamás Sovány, Béla Hopp, Tamás Smausz, Attila Andrásik, Tamás Gera, Zsolt Kovács, Geza Regdon Jr., Anti-counterfeiting protection, personalized medicines- development of 2d identification methods using laser technology, Int. J. Pharm. 605 (2021) 120793.
[10] Sarah J. Trenfield, Hui Xian Tan, Atheer Awad, Asma Buanz, Simon Gaisford, Abdul W. Basit, Alvaro Goyanes, Track-and-trace: novel anti-counterfeit measures for 3d printed personalized drug products using smart material inks, Int. J. Pharm. (ISSN 0378-5173) 567 (2019) 118443, https://doi.org/10.1016/j.ijpharm.2019.06.034, http://www.sciencedirect.com/science/article/pii/S0378517319304776.
[11] Heidi Öblom, Claus Cornett, Johan Bøtker, Sven Frokjaer, Harald Hansen, Thomas Rades, Jukka Rantanen, Natalja Genina, Data-enriched edible pharmaceuticals (deep) of medical cannabis by inkjet printing, Int. J. Pharm. 589 (2020) 119866.
[12] Heyang Zhang, Dawei Hua, Chaobo Huang, Sangram Keshari Samal, Ranhua Xiong, Félix Sauvage, Kevin Braeckmans, Katrien Remaut, Stefaan C De Smedt, Materials and technologies to combat counterfeiting of pharmaceuticals: current and future problem tackling, Adv. Mater. 32 (11) (2020) 1905486.
[13] Ravikanth Pappu, Ben Recht, Jason Taylor, Neil Gershenfeld, Physical one-way functions, Science 297 (5589) (2002) 2026–2030.
[14] Benjamin Willsch, Integration of physically unclonable functions (pufs) in cmos, PhD thesis, Dissertation, Universität Duisburg-Essen, Duisburg, Essen, 2019, 2019.
[15] Yansong Gao, Said F. Al-Sarawi, Derek Abbott, Physical unclonable functions, Nat. Electron. 3 (2) (2020) 81–91.
[16] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, Srinivas Devadas, Physical unclonable functions and applications: a tutorial, Proc. IEEE 102 (8) (2014) 1126–1141.
[17] Zhaoying Hu, Jose Miguel, M. Lobez Comeras, Hongsik Park, Jianshi Tang, Ali Afzali, George S. Tulevski, James B. Hannon, Michael Liehr, Shu-Jen Han, Physically unclonable cryptographic primitives using self-assembled carbon nanotubes, Nat. Nanotechnol. 11 (6) (2016) 559–565.
[18] Yong Geng, JungHyun Noh, Irena Drevensek-Olenik, Romano Rupp, Gabriele Lenzini, Jan P.F. Lagerwall, High-fidelity spherical cholesteric liquid crystal Bragg reflectors generating unclonable patterns for secure authentication, Sci. Rep. 6 (1) (2016) 1–9.
[19] Miguel R. Carro-Temboury, Riikka Arppe, Tom Vosch, Thomas Just Sørensen, An optical authentication system based on imaging of excitation-selected lanthanide luminescence, Sci. Adv. 4 (1) (2018) e1701384.
[20] Jiseok Lee, Paul W. Bisso, Rathi L. Srinivas, Jae Jung Kim, Albert J. Swiston, Patrick S. Doyle, Universal process-inert encoding architecture for polymer microparticles, Nat. Mater. 13 (5) (2014) 524–529.
[21] O. Ivanova, A. Elliott, T. Campbell, C.B. Williams, Unclonable security features for additive manufacturing, Addit. Manuf. 1 (2014) 24–31.
[22] Takao Fukuoka, Yasushige Mori, Toshiya Yasunaga, Kyoko Namura, Motofumi Suzuki, Akinobu Yamaguchi, Physically unclonable functions taggant for universal steganographic prints, Sci. Rep. 12 (1) (2022) 985.
[23] Takao Fukuoka, Toshiya Yasunaga, Kyoko Namura, Motofumi Suzuki, Akinobu Yamaguchi, Plasmonic nanotags for on-dose authentication of medical tablets, Adv. Mater. Interfaces (2023) 2300157.
[24] Alison F. Smith, Paul Patton, Sara E. Skrabalak, Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints, Adv. Funct. Mater. 26 (9) (2016) 1315–1321.
[25] Jangbae Kim, Je Moon Yun, Jongwook Jung, Hyunjoon Song, Jin-Baek Kim, Hyotcherl Ihee, Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires, Nanotechnology 25 (15) (2014) 155303.
[26] Abidin Esidir, Nilgun Kayaci, N. Burak Kiremitler, Mustafa Kalay, Furkan Sahin, Gulay Sezer, Murat Kaya, M. Serdar Onses, Food-grade physically unclonable functions, ACS Appl. Mater. Interfaces 15 (35) (2023) 41373–41384.
[27] Hui Sun, Saurav Maji, Anantha P. Chandrakasan, Benedetto Marelli, Integrating biopolymer design with physical unclonable functions for anticounterfeiting and product traceability in agriculture, Sci. Adv. 9 (12) (2023) eadf1978.
[28] Hee-Jae Jeon, Jung Woo Leem, Yuhyun Ji, Sang Mok Park, Jongwoo Park, Kee-Young Kim, Seong-Wan Kim, Young L. Kim, Cyber-physical watermarking with inkjet edible bioprinting, Adv. Funct. Mater. 32 (18) (2022) 2112479.

[29] Jung Woo Leem, Hee-Jae Jeon, Yuhyun Ji, Sang Mok Park, Yunsang Kwak, Jongwoo Park, Kee-Young Kim, Seong-Wan Kim, Young L. Kim, Edible matrix code with photogenic silk proteins, ACS Cent. Sci. 8 (5) (2022) 513–526.
[30] Elizabeth A. Clark, Morgan R. Alexander, Derek J. Irvine, Clive J. Roberts, Martin J. Wallace, Sonja Sharpe, Jae Yoo, Richard J.M. Hague, Chris J. Tuck, Ricky D. Wildman, 3d printing of tablets using inkjet with uv photoinitiation, Int. J. Pharm. 529 (1–2) (2017) 523–530.
[31] Ivan Rehor, Sophie van Vreeswijk, Tina Vermonden, Wim E. Hennink, Willem K. Kegel, Huseyin Burak Eral, Biodegradable microparticles for simultaneous detection of counterfeit and deteriorated edible products, Small 13 (39) (2017) 1701804.
[32] Daniel Krewski, Melvin E. Andersen, Michael G. Tyshenko, Kannan Krishnan, Thomas Hartung, Kim Boekelheide, John F. Wambaugh, Dean Jones, Maurice Whelan, Russell Thomas, et al., Toxicity testing in the 21st century: progress in the past decade and future perspectives, Arch. Toxicol. 94 (2020) 1–58.
[33] Yuanhui Zheng, Cheng Jiang, Soon Hock Ng, Yong Lu, Fei Han, Udo Bach, J. Justin Gooding, Unclonable plasmonic security labels achieved by shadow-mask-lithography-assisted self-assembly, Adv. Mater. 28 (12) (2016) 2330–2336.
[34] Kae Jye Si, Debabrata Sikdar, Lim Wei Yap, Jeremy Kee Keong Foo, Pengzhen Guo, Qianqian Shi, Malin Premaratne, Wenlong Cheng, Dual-coded plasmene nanosheets as next-generation anticounterfeit security labels, Adv. Opt. Mater. 3 (12) (2015) 1710–1717.
[35] U. Korcan Demirok, Jared Burdick, Joseph Wang, Orthogonal multi-readout identification of alloy nanowire barcodes, J. Am. Chem. Soc. 131 (1) (2009) 22–23.
[36] Minye Yang, Ying Zhang, Meihui Cui, Yu Tian, Shufang Zhang, Kang Peng, Hongshuang Xu, Zhenyu Liao, Hanjie Wang, Jin Chang, A smartphone-based quantitative detection platform of mycotoxins based on multiple-color upconversion nanoparticles, Nanoscale 10 (33) (2018) 15865–15874.
[37] Alan Wee-Chung Liew, Hong Yan, Mengsu Yang, Pattern recognition techniques for the emerging field of bioinformatics: a review, Pattern Recognit. 38 (11) (2005) 2055–2073.
[38] Stefan Johansen, Michal Radziwon, Luciana Tavares, Horst-Günter Rubahn, Nanotag luminescent fingerprint anti-counterfeiting technology, Nanoscale Res. Lett. 7 (1) (2012) 1–5.
[39] Priyanka Sharma, Manavjeet Kaur, Classification in pattern recognition: a review, Int. J. Adv. Res. Comp. Sci. Softw. Eng. 3 (4) (2013).
[40] Guosheng Tang, Long Chen, Zixuan Wang, Shuting Gao, Qingli Qu, Ranhua Xiong, Kevin Braeckmans, Stefaan C. De Smedt, Yu Shrike Zhang, Chaobo Huang, Faithful fabrication of biocompatible multicompartmental memomicrospheres for digitally color-tunable barcoding, Small 16 (24) (2020) 1907586.
[41] Ketie Saralidze, Leo H. Koole, Menno L.W. Knetsch, Polymeric microspheres for medical applications, Materials 3 (6) (2010) 3537–3564.
[42] K. Krutkramelis, B. Xia, J. Oakey, Monodisperse polyethylene glycol diacrylate hydrogel microsphere formation by oxygen-controlled photopolymerization in a microfluidic device, Lab Chip 16 (8) (2016) 1457–1465.
[43] Guosheng Tang, Ranhua Xiong, Dan Lv, Ronald X. Xu, Kevin Braeckmans, Chaobo Huang, Stefaan C. De Smedt, Gas-shearing fabrication of multicompartmental microspheres: a one-step and oil-free approach, Adv. Sci. 6 (9) (2019) 1802342.
[44] Stefano Sacanna, Mark Korpics, Kelvin Rodriguez, Laura Colón-Meléndez, Seung-Hyun Kim, David J. Pine, Gi-Ra Yi, Shaping colloids for self-assembly, Nat. Commun. 4 (1) (2013) 1–6.
[45] MathWorks, Imfindcircles description, http://nl.mathworks.com/help/images/ref/imfindcircles.html, 2015.
[46] Omprakash Patel, Yogendra P.S. Maravi, Sanjeev Sharma, A comparative study of histogram equalization based image enhancement techniques for brightness preservation and contrast enhancement, arXiv preprint arXiv:1311.4033, 2013.
[47] Weidong Zhang, Peixian Zhuang, Hai-Han Sun, Guohou Li, Sam Kwong, Chongyi Li, Underwater image enhancement via minimal color loss and locally adaptive contrast enhancement, IEEE Trans. Image Process. 31 (2022) 3997–4010.
[48] Yuan-Kai Huo, Gen Wei, Yu-Dong Zhang, Le-Nan Wu, An adaptive threshold for the canny operator of edge detection, in: 2010 International Conference on Image Analysis and Signal Processing, IEEE, 2010, pp. 371–374.
[49] Heider AM Wahsheh, Mohammed S. Al-Zahrani, Secure and usable qr codes for healthcare systems: the case of covid-19 pandemic, in: 2021 12th International Conference on Information and Communication Systems (ICICS), IEEE, 2021, pp. 324–329.
[50] Anthony Van Herrewege, Stefan Katzenbeisser, Roel Maes, Roel Peeters, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, Christian Wachsmann, Reverse fuzzy extractors: enabling lightweight mutual authentication for puf-enabled rfids, in: Financial Cryptography and Data Security: 16th International Conference, FC 2012, Revised Selected Papers 16, Kralendijk, Bonaire, Februray 27–March 2, 2012, Springer, 2012, pp. 374–389.
[51] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Technical report, Booz Allen & Hamilton, 2001.
[52] Carmina Georgescu, Emil Simion, Alina-Petrescu Nita, Antonela Toma, A view on nist randomness tests (in)dependence, in: 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2017, pp. 1–4.
[53] Andrew L. Rukhin, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2010.
[54] Abhranil Maiti, Vikash Gunreddy, Patrick Schaumont, A systematic method to evaluate and compare the performance of physical unclonable functions, in: Embedded Systems Design with FPGAs, Springer, 2013, pp. 245–267.