Authentication of Optical Physical Unclonable Functions Based on Single-Pixel Detection

Pidong Wang,1,2,* Feiliang Chen,1,2 Dong Li,1,2 Song Sun,1,2 Feng Huang,1,2 Taiping Zhang,1,2 Qian Li,1,2 Kun Chen,1,2 Yongbiao Wan,1,2 Xiao Leng,1,2 and Yao Yao1,2,†

1Microsystem and Terahertz Research Center, China Academy of Engineering Physics, Chengdu 610200, China
2Institute of Electronic Engineering, China Academy of Engineering Physics, Mianyang 621999, China

(Received 6 May 2021; revised 17 September 2021; accepted 15 October 2021; published 11 November 2021)

Physical unclonable function (PUF) has been proposed as a promising and trustworthy solution to a variety of cryptographic applications. Here we propose a nonimaging-based authentication scheme for optical PUFs materialized by random scattering media, in which the characteristic fingerprints of optical PUFs are extracted from stochastical fluctuations of the scattered light intensity with respect to laser challenges, which are detected by a single-pixel detector. The randomness, uniqueness, unpredictability, and robustness of the extracted fingerprints are validated to be qualified for real authentication applications. By increasing the key length and improving the signal-to-noise ratio, the false accept rate of a fake PUF can be dramatically lowered to the order of $10^{-28}$. In comparison to the conventional laser-speckle-imaging-based authentication with unique identity information obtained from textures of laser-speckle patterns, this nonimaging scheme can be implemented at small speckle size bellowing the Nyquist–Shannon sampling criterion of the commonly used CCD or CMOS cameras, offering benefits in system miniaturization and immunity against reverse engineering attacks simultaneously.

DOI: 10.1103/PhysRevApplied.16.054025

I. INTRODUCTION

Physical unclonable functions (PUFs) are physical entities with unique security behaviors, which make them ideal in the field of hardware security [1–6]. The uncontrollable nature of complex random disorders inside PUFs, which appear during the manufacturing process, makes duplication of them impractical or at such an expensive cost, which renders it worthless [7,8]. Optical PUF, composed of bulk random scattering media [9–13], thin random scattering layer (such as regular paper [14]) or rough scattering surface (such as laser-engraved surface [7,15]), is a subset of PUFs of particular interest. The huge number, small size, and random distribution of dense micro- and nanostructures inside or on the surface of an optical PUF make it highly informative, resource efficient, intrinsically tamper resistant, inexpensive to fabricate, but difficult or too costly to duplicate [9–11,16–18]. Moreover, with mature image-based feature-extraction methods, the fingerprint information of optical PUFs could be easily accessed from textures of laser-speckle patterns, which are derived from mutual interference of randomly scattered laser light from the surface and inside of optical PUFs and thus are especially favorable in three-dimensional (3D) random physical feature exploration [9,10,19–23]. These perfect characters render optical PUF excellent in entity authentication.

Unfortunately, the development of reverse-engineering techniques poses severe threat to optical PUFs. For example, nanoscale synchrotron x-ray computed tomography (SXCT) and 3D nanoprinting are now capable of achieving spatial resolution down to tens of nanometers and are still in rapid development [24–29], which makes it, in principle, possible to accurately capture the precise nanostructure of an optical PUF and even reproduce it, especially for those composed of random rough surface. Thus it is necessary to increase the degree of complexity or cost of resources against the reverse-engineering attacks on optical PUFs.

Taking into consideration the speed and resource cost of reverse-engineering techniques, it is favorable to achieve the goal by simply increasing the effective volume of an optical PUF, namely increasing its actually illuminated region. Since the thickness would affect both transmittance of laser light and angular sensitivity of laser speckle for bulk and layered scattering media [30–34], it is better to increase the effective volume via increasing the optical illumination area for optical PUFs composed of bulk and layered materials, just the same as optical PUFs composed of a rough scattering surface. However, since the mean speckle size of a laser-speckle pattern is proportional to $z/d$, where $z$ is the distance of the camera from the optical...
PUF and \( d \) is the size of the laser illumination area \([35]\), the speckle will be comparable to or even smaller than the pixel of commonly used CCD or CMOS cameras when the laser illumination area is large enough, resulting that the speckle pattern will be averaged out and can not be clearly observed \([36]\). On the other hand, as system miniaturization is always on demand, the camera for laser-speckle pattern observation is expected to be mounted as close to the optical PUF as possible, namely the value of \( z \) is expected to be as small as possible, which would also lead to fuzzy imaging of laser-speckle patterns. Consequently, it will be difficult to evaluate characteristic random features and extract identity information of an optical PUF from textures of laser-speckle patterns, which would make conventional laser-speckle-imaging-based authentication of optical PUFs impractical. Therefore, a nonimaging-based scheme applicable at small speckle size is imperative for highly secure integrated authentication of optical PUFs.

In this work, we propose a nonimaging-based authentication scheme for optical PUFs executable at small speckle size, in which response signals of optical PUFs are detected by a single-pixel detector. We first theoretically and experimentally validate the feasibility of fingerprint information accession from single-pixel detected stochastic fluctuations of the scattered light with respect to challenges under the circumstance of small-sized laser speckles, which are fuzzy to the commonly used CCD or CMOS cameras. Randomness, uniqueness, unpredictability, and robustness of the binary keys generated from the fluctuations are statistically evaluated for the necessary requirements of authentication applications. The method for reduction of the false acceptance rate (FAR) and false rejection rate (FRR) in authentication is also discussed, as well as its positioning accuracy requirement. At last an associated authentication protocol implementable at small speckle size is designed. Compared to the conventional laser-speckle-imaging-based authentication with identity information extracted from textures of laser-speckle patterns, such a nonimaging scheme leverages the advantage of small speckles and thus is advantageous in increasing both the security against reverse-engineering attacks and the integration degree of the application units at the same time.

II. AUTHENTICATION SETUP AND PRINCIPLES

A schematic for the authentication setup is shown in Fig. 1. An expanded and collimated helium-neon laser beam illuminates on a binary amplitude digital micromirror device (DMD) to encode the beam by shaping the laser wave front with randomly configuring the reflection pattern of the DMD, namely randomly setting the reflection coefficient \( r_k \) \((r_k = 0 \text{ or } 1)\) of each DMD pixel. In the methodology of PUF-based authentication protocols, such an encoded wave front corresponding to each DMD configuration is usually referred to as a “challenge” \([9,12]\). A lens, \( L_1 \), Fourier transforms the encoded beam and an iris in its Fourier plane blocks all the diffraction orders except the \(-1\)st, which carries all the encoded information of the beam \([37–39]\). Passing through another lens \( L_2 \), the encoded beam (i.e., challenge) is projected onto the surface of the PUF to stimulate it. After complex interactions with the optical PUF, the scattered light is detected by a single-pixel photon detector in the far field. We show that the detected light, even at small speckle size, will fluctuate with the variation of challenges and can be treated as the response signal to the challenge in authentication applications.

The electric field of the scattered light at a point \( r \) on the surface of the detector can be calculated by \([40,41]\)

\[
E(r) = \sum_{k=1}^{m} t_k \cdot r_k \cdot E_{in}^k, \tag{1}
\]

where \( k \) and \( m \) are the index and the total number of DMD pixels, respectively; \( E_{in}^k \) is the light electric field at the incident surface of the PUF; \( r_k \) is the reflection coefficient of the \( k \)th DMD pixel, which follows an equiprobable Bernoulli distribution to get the maximum randomness (i.e., \( r_k \) is set to be 0 or 1 with equal probability); \( t_k = |t_k| \cdot e^{i\phi_k} \) describes the transfer of \( E_{in}^k \) to the point \( r \), where the amplitude \(|t_k|\) is Rayleigh distributed and the phase \( \phi_k \) is uniformly distributed in the interval \([-\pi, \pi]\) \([42,43]\).

As the random nature of \( t_k \), the electric field of the scattered light, as well as the corresponding light intensity, will fluctuate stochastically with random modulations of \( r_k \). Moreover, it could be noted that Eq. (1) shares almost the same form as the function used by Goodman to calculate the electric field inside a single speckle pattern \([35]\), except that the electric field of Eq. (1) changes with the modulation of \( r_k \) while the electric field inside a single speckle pattern varies with the observation point.
Therefore, following the same derivation steps as Goodman [35], it can be concluded from Eq. (1) that the fluctuation of the single-pixel detected intensity of the scattered light follows the gamma distribution:

\[ p_{\alpha}(I_\alpha) = \frac{1}{\Gamma(\mu)} \left( \frac{\mu}{I_\alpha} \right)^\mu I_\alpha^{\mu-1} \exp\left( -\frac{\mu I_\alpha}{I_\alpha} \right). \]  

(2)

Here \( I_\alpha = \iint_{r\in \mathbb{R}^2} |E(r)|^2 dr \) is the integrated light intensity over the active area \( \alpha \) of the detector. The angular brackets \( \langle \cdots \rangle \) denote an average over the ensemble of random challenges and thus \( \langle I_\alpha \rangle \) is the mean intensity detected by the single-pixel detector. \( \Gamma(\mu) \) represents the gamma function. \( \mu \) is the characteristic shape parameter of the gamma distribution and its value depends on the size of the speckle: for speckles with average diameter larger than the size of the detector, \( \mu \approx 1 \), meaning that \( I_\alpha \) approaches the negative exponential distribution, while in the opposite case, namely for speckles with average diameter smaller than the size of the detector, \( \mu > 1 \), implying that \( I_\alpha \) follows the gamma distribution. As a result, the signal detected by the single-pixel detector will fluctuate stochastically with respect to the randomly encoded challenges regardless of what the size of the speckle is, and the speckle size affects only the shape of the distribution.

In our experiment we have access to the photon number of the scattered light. The number of photons \( N \) detected by the single-pixel photon detector in a time interval of \( \Delta t \) is equal to \( I_\alpha \times \Delta t / h \omega \), where \( \omega \) is the angular frequency of the challenge beam and \( h \) is the reduced Planck constant. Thus \( N \) is also gamma distributed, and its distribution can be written as

\[ p_N(N) = p_{\alpha} \langle N h\omega / \Delta t \rangle \times \frac{\partial}{\partial N} I_\alpha \]

\[ = \frac{1}{\Gamma(\mu)} \left( \frac{\mu}{N} \right)^\mu N^{\mu-1} \exp\left( -\frac{\mu N}{N} \right). \]  

(3)

where \( \langle N \rangle = \langle I_\alpha \rangle \times \Delta t / h \omega \) is the mean photon number. Thus the photon number \( N \) follows the same fluctuation behavior as \( I_\alpha \).

Equations (1)–(3) indicate that the detected signals \( I_\alpha \) and \( N \) are related to both the physical features of the optical PUF and the parameters of the challenge light (\( |E_{in}^k| \) and \( r_k \)). To eliminate the impact of the challenge light intensity, \( |E_{in}^k| \) should keep approximately equal at each pixel and constant during the detection, besides, the number of reflecting DMD pixels (\( \sum_{k=1}^{m} r_k \)) should also be fixed. As a result, the fluctuation of the detected signal is only related to the binary reflection patterns displayed on the DMD, namely the encoded information, and the physical features of the PUF. Hence the fluctuation can be regarded as a unique response (i.e., fingerprint) of a specific PUF to a specific challenge sequence, and based on it the authentication can be implemented.

Moreover, being the same with laser speckle, the fluctuation is also induced by mutual interference of randomly scattered light coming from micro- and nanostructures both inside and on the surface of the optical PUF, thus it retains the advantage of laser speckle in easy exploration of 3D physical information.

### III. EXPERIMENTAL DEMONSTRATION

#### A. Stochastic fluctuations of the scattered light and binary key generation

Our optical PUFs are fabricated by titania (TiO\(_2\)) nanoparticles with an average grain size of 200 nm randomly immersed in PMMA films of thickness about 17 \( \mu m \). Their transport mean free path is measured to be approximately 1.3 \( \mu m \) by coherent backscattering experiment [44], which implies that a photon will be scattered 13 times on average to transport through the film, leading the PUF to be a multiple scattering media [45–47]. The diameter of the incident beam is about 4 cm, which is large enough to cover the full active area of the DMD (Vialux V-7001). The beam reflected by the DMD encoding area is rectangular in shape with a length-to-width ratio of 4:3. Figure 2(a) plots the mean speckle size \( D \) versus the distance \( z \) between the optical PUF and the CCD camera (Thorlabs 340M-USB, with a pixel size of 7.4 \( \times \) 7.4 \( \mu m^2 \)), as well as the width of the incident beam \( d \), which is controlled by adjusting the width of the encoding area of the DMD (i.e., the width of the DMD reflection pattern). The

![Figure 2](image-url)  
**FIG. 2.** (a) Mean speckle size \( D \) versus \( z \) and \( d \), which are the distance from the optical PUF to the CCD camera and the width of the rectangular incident challenge beam, respectively. White dashed line corresponds to the minimum Nyquist–Shannon sampling size. (b)–(d) Speckle patterns observed at points \( O, P, \) and \( Q \), respectively.
size around the white dashed line is about twice the camera’s pixel size, which is the minimum Nyquist-Shannon sampling size. In the area below the white dashed line, the speckle size is evaluated by calculating the width of the normalized autocorrelation function of the intensity pattern of the speckle [48, 49], while in the area above, it is evaluated by surface extrapolating from data below the white dashed line using the formula $D \propto z/d$ [35], owing to the fact that the speckles in this area are so small that they could not be observed clearly by the camera. It can be seen that the mean size of the speckle increases with $z$ and decreases with $d$.

For illustration purpose, Figs. 2(b) and 2(c) show two speckle patterns recorded at points $O$ ($z = 35$ mm and $d = 0.66$ mm) and $P$ ($z = 130$ mm and $d = 2.16$ mm), respectively, inside which textures of laser speckles can be observed clearly and are of moderate speckle size for laser-speckle-imaging-based authentication. The almost same mean speckle size in these two figures indicates that the camera’s distance to the optical PUF should be increased with the illumination area simultaneously in order that the mean speckle size remains unchanged, implying that we cannot increase the effective volume of an optical PUF without changing the size of a laser-speckle-imaging-based authentication system. Figure 2(d) records a speckle pattern at point $Q$ ($z = 35$ mm and $d = 2.16$ mm), which is of the same camera’s distance to the optical PUF as point $O$ and of the same illumination area as point $P$, and inside the figure speckles are of small mean size of only approximately 1.36 times the camera pixel size, which is much smaller than the minimum Nyquist-Shannon sampling size. Point $Q$ has both large illumination area and short camera distance to the optical PUF, nevertheless, textures of the speckle patterns at this point are so fuzzy to the camera that they are not applicable for laser-speckle-imaging-based authentication.

To detect the fuzzy speckle response at point $Q$, the camera is replaced by a single-pixel photon detector with an active area of $180 \mu$m in diameter (Excelitas SPCM-AQRH-14). When a photon is detected, the detector will output a transistor-transistor logic (TTL) pulse, and we exploit a data-acquisition card (NI USB-6351) to count the number of the outputted TTL pulses, i.e., the number of detected photons. The DMD encoding area consisting of $960 \times 720$ pixels is divided into $40 \times 30$ segments to shape the beam wave front, each of which consists of $24 \times 24$ pixels and acts as a superpixel for amplitude modulation of the incident wave front. In order to get a challenge of a fixed amount of reflecting segments while with the maximum randomness, half of the segments are randomly chosen and set to 1, allowing a maximum of $1200 \times 600 \approx 10^{360}$ distinguishable challenges. The Shannon entropy of each bit in a challenge is equal to $\frac{1}{2} \log_2(\frac{1}{2}) - \frac{1}{2} \log_2(\frac{1}{2}) = 1$ bit, which is the maximum entropy of a binary bit, indicating that the challenges are incompressible and hard to predict [50, 51]. Fluctuations of the scattered photon numbers are subsequently measured by the single-pixel photon detector when illuminating a PUF with randomly modulated challenges during a time interval of 1 ms. (b) Distribution of the detected photons. (c) Two 150-bit binary barcode key tags. (d) The probability of each of the bits being set to 1 (red line), calculated by averaging over an ensemble of 1000 bits of different encoded challenges. The blue line graphs the Shannon entropy.

By comparing with a comparison threshold, binary keys can be generated from the detected fluctuating signals. Figure 3(c) shows two one-dimensional (1D) 150-bit barcode key tags generated from points in the red dashed box in Fig. 3(a) with the comparison threshold equaling the median value of the detected photon numbers, i.e., 2435, as the red dashed line plots in Figs. 3(a) and 3(b). Figure 3(d) presents the influence of the comparison threshold value, in which the average probability of a bit being set to 1 is equal to 0.5 and the Shannon entropy [10] reaches its maximum when the comparison threshold approaches the median.
value of the detected fluctuating photon numbers, implying that binary numbers with bitwise maximum entropy are produced at this point. Therefore, in the ensuing discussion, the comparison threshold for binary key generation is set to the median value \(N_m\) of the detected response signals of each PUF.

### B. Statistical properties of the generated binary keys

To enable the usage of optical PUFs with single-pixel detection of response signals in authentication applications, it is necessary to carefully evaluate randomness, uniqueness, unpredictability, and robustness of the detected response signals \([2,4]\).

Here the randomness of binary numbers generated from the stochastically fluctuating photon numbers detected at point \(Q\) in Fig. 2(a) is tested by a standard National Institute of Standards and Technology (NIST) randomness test suite \([52]\). The length of the used binary number sequence for the first 15 benchmarks of NIST test (i.e., all except “Random excursions” and “Random excursions variant”) is 10.000, while the length for the last two benchmarks (i.e., “Random excursions” and “Random excursions variant”) is 1000.000. Each of the NIST test benchmarks is repeated 100 times. Table I shows the results of the NIST test, and it confirms that the generated binary numbers successfully pass the NIST randomness tests, i.e., the probability value \((P\) value\) is greater than 0.01 and the uniformity exceeds 0.0001 \([52–54]\). We also evaluate the randomness of binary numbers generated from Fig. 2(d) by comparing the intensity at each pixel with the median intensity of the whole picture, but they fail to pass the NIST test, because the intensities between the adjacent pixels are correlated \([10,55]\). Consequently, if parallel detection with multiple detectors is used to improve the generation speed and efficiency of binary numbers, as well as to reduce the number of challenges required for the generation of binary keys of a fixed length, detectors should be mounted far enough between each other.

To evaluate the uniqueness, unpredictability, and robustness of the detected response signal, binary keys of a fixed length of \(L\) bits generated from the stochastically fluctuating photon numbers detected at point \(Q\) in Fig. 2(a) are statistically analyzed by calculating the normalized Hamming distance (HD) among them, which counts the percentage of bits that differ between two keys. Here two kinds of inter-HDs are calculated: inter-HDs among keys generated by illuminating different PUFs with the same challenge sequence (inter-HD I), and inter-HDs among keys generated by illuminating the same PUF with different challenge sequences (inter-HD II). Inter-HD I assesses the uniqueness of a binary key to its generating PUF, while inter-HD II evaluates the uniqueness of a binary key to its generating challenge sequence and the unpredictability of the binary key. The red and orange histograms in Fig. 4 plot the distributions of inter-HD I and inter-HD II, respectively, both of which are calculated among 50 150-bit binary keys. The two inter-HDs share the same distribution and both can be well fitted by a modified binomial distribution:

\[
f(x) = \binom{L}{[L \times x]} p^x (1-p)^{L-[L \times x]},
\]

as the olive fitting curve in Fig. 4 shows. Here \(x\) is the normalized HD and the rounded number \(L \times x\) represents the number of bits that differ in two different keys. The parameter \(p\) represents the mean normalized HD. The resulting distributions of the two inter-HDs have the same mean of approximate 0.496, which means an almost even odds of a bit to be different, implying that a binary key is unique not only to its generating PUF but also to the challenge sequence and it is unpredictable. The variances of the two histograms are equal to 1.67 x 10^{-3}, so there are 0.496 x (1 - 0.496)/1.67 x 10^{-3} \approx 150 independent identically distributed variables in the binary key, which represents that all the bits in the binary key are independent identically distributed and a theoretical key space size on the order of \(2^L\) distinguishable \(L\)-bit binary keys can be provided by the PUF.

The robustness of the generated binary keys is estimated with HDs among remeasured copies of a binary key, labeled as intra-HD. The blue histograms in Fig. 4 show the distribution of the intra-HD among 50 remeasured copies of a 150-bit binary key, and it can be well fitted by the modified binomial distribution \([\text{Eq. } (4)]\), as indicated by the green fitting curve. The mean value of intra-HD is

\[
\text{TABLE I. Results of the NIST randomness test.}
\]

| Test type                        | Uniformity of \(P\) value | Pass rate (%) |
|----------------------------------|---------------------------|---------------|
| Frequency                        | 0.554                     | 100           |
| Frequency test within a block    | 0.616                     | 98            |
| Runs                             | 0.290                     | 97            |
| Longest run of ones in a block   | 0.494                     | 97            |
| Binary matrix rank               | 0.213                     | 100           |
| Discrete Fourier transform       | 0.616                     | 99            |
| Nonoverlapping template matching | 0.0026\(^a\)              | 96            |
| Overlapping template matching    | 0.679                     | 99            |
| Universal                        | 0.740                     | 99            |
| Linear complexity                | 0.038                     | 99            |
| Serial                           | 0.419                     | 99            |
| Serial                           | 0.924                     | 99            |
| Approximate entropy              | 0.052                     | 99            |
| Cumulative sums—forward          | 0.350                     | 100           |
| Cumulative sums—backward         | 0.437                     | 100           |
| Random excursions                | 0.052\(^a\)              | 97.67         |
| Random excursions variant        | 0.027\(^a\)              | 97.67         |

\(^a\) More than one value is obtained and the values given for these tests are their minimum.
0.056 and its variance is $3.6 \times 10^{-4}$. The nonzero mean value demonstrates that the same PUF even mounted at the same place and illuminated by the same challenge sequence rarely produces completely identical binary keys. This is caused by system noises, including photon shot noise, intensity noise of the laser, dark current noise of the photon detector, light pollution in the environment, etc.

Nevertheless, the almost zero mean distance indicates that there are only a few bits (about 8 bits on average) differ in their remeasured copies, thus the binary key is robust and retrievable.

As the random, unique, unpredictable, and robust nature, the generated binary keys can be regarded as fingerprints to optical PUFs and are qualified for authentication applications. Moreover, due to the large space size of challenge and response and the uniqueness of a binary key to its corresponding challenge sequence, it is possible to use each binary key only once, which could greatly improve the security of the authentication [9].

C. Authentication with the generated binary keys

Based upon the above statistical analysis, authentication can be implemented. To decide whether a candidate PUF is the right one previously enrolled in the database in authentication, the minimum probability-of-error decision rule is to reject the candidate when the probability that the two PUFs are the same is less than the probability that they are different [9]. The two fitting curves in Fig. 4 intersect at $x_c \approx 0.221$, so we can arrive at a decision rule to reject a PUF’s authenticity if the $L$-bit binary key differ by more than $x_c \times L = 0.221 \times 150 \approx 33$ bits.

Due to the fact that point $Q$ in Fig. 2(a) has both large illumination area and short detector distance to the optical PUF, authentication based on single-pixel detection of response signals at this point is performed with a large effective volume of the optical PUF and a high integration level of the authentication system at the same time. And further it can be expected that the authentication can still be implemented even with the effective volume expanding to a far larger extent and the detector mounted far closer to the optical PUF than point $Q$, hence the single-pixel-detection-based authentication can be implemented far more safely and compactly in respect to conventional laser-speckle-imaging-based authentication.

D. Reduction of FAR and FRR

Since there is always a small overlap between the distribution of inter-HDs and intra-HDs around the intersection point $x_c$, false acceptance of a fake PUF and false rejection of a true PUF might occur, especially for cases of HDs close to $x_c$. From this perspective, the authentication of a candidate PUF can be viewed as a fundamental problem of statistical inference, that is, binary hypothesis testing (i.e., true or fake of a candidate PUF) [56]. In this context, FRR and FAR (also known as type-I and type-II errors in statistical inference [56]), which count the probabilities of the false rejection and the false acceptance, respectively, are necessary to estimate the security of the authentication result [9]. FAR and FRR can be calculated by the following cumulative function:

$$
\begin{align*}
P_{FR} &= 1 - F \left( \left[ L \times x_c \right] , L, p_1 \right) \\
P_{FA} &= F \left( \left[ L \times x_c \right] , L, p_2 \right)
\end{align*}
$$

Here $P_{FR}$ and $P_{FA}$ represent FRR and FAR, respectively. $F \left( \left[ L \times x_c \right] , L, p_i \right) = \sum_{j=0}^{\left[ L \times x_c \right]} \left( \begin{array}{c} L \\ j \end{array} \right) p_i^j (1 - p_i)^{L-j}, i = 1 \text{ or } 2$, which is the cumulative distribution function of the binomial distribution. The parameters $p_1$ and $p_2$ are the mean values of intra-HD and inter-HD I, respectively. Therefore, we can arrive at a FAR of $6.3 \times 10^{-12}$ and a FRR of $2.1 \times 10^{-12}$ in the case of Fig. 4.

In real applications, it is useful to reduce the FAR and FRR for the security of authentication. The statistical results in Fig. 4 illustrate that there are two effective ways to reduce FAR and FRR: reducing the variance of each distribution, and increasing the difference between $p_1$ and $p_2$.

As the variance of the normalized HD is equal to $p_i(1 - p_i)/L$ [9], $i = 1 \text{ or } 2$, FAR and FRR can be lowered by increasing the key length $L$. Figures 5(a) and 5(b) plot the influence of the key length $L$ on the mean values of the normalized HDs and their corresponding variances, which illustrate that not only the mean intra-HD $p_1$ but also the variances of both histograms are successfully decreased. Figure 5(c) shows that FAR and FRR are successfully lowered when increasing the key length, and they both can be well approximated by a simple decaying exponential.

As mentioned above, the mean intra-HD $p_1$ is affected by many kinds of noises, hence it is possible to increase the SNR of the detected signal to lower the value of $p_1$ so as to increase the difference between $p_1$ and $p_2$. An effective
and commonly used method to increase SNR is to increase the strength of the signal. To adopt this method here, the generated binary keys should be invariant to the intensity of the scattered light. The median value (i.e., comparison threshold for binary key generation) of the detected photon numbers \( N_m \) can be calculated by the following equation:

\[
0.5 = \sum_{N=0}^{N_m} p_1(N),
\]

\[
= \frac{1}{\Gamma(\mu)} \mu^{\mu} \sum_{N=0}^{N_m} \left( \frac{N}{\langle N \rangle} \right)^{\mu-1} \exp \left( -\mu \times \frac{N}{\langle N \rangle} \right) ,
\]

which implies that \( N_m / \langle N \rangle \) is a constant irrelevant to the value of \( \langle N \rangle \). The ratio of the detected signal to its mean value can be calculated by \( N / \langle N \rangle = \int \alpha \sum_{k=1}^{m} r_k \times |t_k|^2 \times dr / \left( \int \alpha \sum_{k=1}^{m} r_k \times |t_k|^2 \times dr \right) \), which is also a constant value for each challenge. So \( N/N_m \) would be a constant value for each challenge under arbitrary mean scattering intensity, as well as under arbitrary median scattering intensity, as long as the mean and median intensity keep invariant during the key production. Therefore, increasing the intensity of the scattered light will not affect the binary key generation and can be used to increase the SNR here. Figures 5(d) and 5(e) plot the change of the mean normalized HDs and their corresponding variances with respect to the median value of the detected photon numbers. It can be seen that not only the value of \( p_1 \) but also its corresponding variance are successfully decreased. Figure 5(f) shows that FAR and FRR are successfully lowered with increasing \( N_m \), and they can be well approximated by a decaying polynomial.

Another way to reduce the impact of noise is to discard those challenges with scattering intensities close to the comparison threshold, thus only response signals with high SNR are remained and stored. As indicated in Fig. 3(a), points inside the red area (i.e., points between \( N_m - \delta \) and \( N_m + \delta \), where \( \delta \) is half the height of the red area) are discarded. Figures 5(g) and 5(h) plot the change of the mean normalized HDs and their corresponding variances with the value of \( \delta \), in which the value of \( p_1 \) and its corresponding variance are also successfully decreased with increasing the value of \( \delta \). The FAR and FRR also decrease approximately exponentially as shown in Fig. 5(i), but there is a threshold around 0.032\( N_m \) for \( \delta \), where the decay rate at \( \delta > 0.032 N_m \) is smaller than that at \( \delta < 0.032 N_m \). This is caused by the elimination of all of the noise except the photon shot noise. After optimization by increasing the

![Figure 5](image-url)

**FIG. 5.** (a)–(c) Mean normalized HD, variance, FAR and FRR versus the key length, respectively (\( N_m = 2429, \delta = 0 \)). (d)–(f) Mean normalized HD, variance, FAR and FRR versus the \( N_m \), respectively (\( L = 150, \delta = 0 \)). (g)–(i) Mean normalized HD, variance, FAR and FRR versus the value of \( \delta \), respectively (\( L = 150, N_m = 2429 \)). Red and blue lines in (c),(f), and (i): fitting curves of FAR and FRR, respectively.
SNR, including increasing the intensity of the scattered light and discarding responses with low SNR, the security parameter FAR can be lowered even to the order of $10^{-28}$ for authentication with a key length of 150 bits.

Based on the theoretical analysis in Sec. II, the response signal detected by the single-pixel detector will fluctuate no matter what the size of the speckle is, and the speckle size affect only the line shape of the statistical distribution of the fluctuation, so the single-pixel detection scheme would still be feasible even for a speckle pattern with speckle size of submicron or subwavelength. However, our present experiment shows that the fluctuation will be overwhelmed by noise with continuing reduction of the speckle size to such an extent, so seeking methods to lower the SNR is necessary to validate the scheme in the submicron and subwavelength region.

E. Positioning accuracy requirement of optical PUF

In authentication applications, optical PUFs would be repeatedly removed and reinserted into the light path, so the plug and play mount for the optical PUF should own a precise repeatability of position for the retrieval of response signals [9,10,12,31]. In Figs. 6(a) and 6(b), the laser beams are successively translated and rotated about the PUF by a small amount of $dx$ and $d\theta$ respectively, which shows that a translation of approximate 30 $\mu$m or a rotation of approximate $0.5^\circ$ will cause the generated binary keys to decorrelate completely. Therefore, commercial products, such as Thorlabs KB1X1, whose position error is smaller than 2.5 $\mu$m and 26.72 $\mu$rad, is precise enough for the positioning of optical PUFs in authentication applications.

IV. AUTHENTICATION PROTOCOL

Given the preceding analysis, the generated binary keys, extracted from single-pixel detection of small-sized laser speckle response, are random, unique, unpredictable, and robust enough for authentication applications. A simple authentication protocol is shown in Fig. 7, in which the execution can be divided into two steps: enrollment and verification.

**Enrollment stage.** A large number of challenges ($C_i$) randomly encoded by the DMD are sent to illuminate an optical PUF and their corresponding scattered light are detected by a single-pixel detector. Comparing with the median value, the detected signals are transformed into binary numbers ($R_i$). Challenges together with their corresponding binary responses are recorded to form challenge-response pairs ($C_i - R_i$), and then stored into a challenge-response database.

**Verification**. A new challenge ($C_j$) is sent to the PUF, and the corresponding scattered light is detected by the single-pixel detector. The detected binary number ($R_j$) is compared with the recorded challenge-response pairs. If $HD(K_u, K_j) < x_c$, the key is considered to be genuine; otherwise, it is considered to be fake.

FIG. 6. (a) Translational sensitivity of the key. (b) Rotational sensitivity of the key. $L = 150, N_m = 2429, \delta = 0$.

FIG. 7. Authentication protocol based on single-pixel detection of response signals.
Verification stage. $L$ challenge-response pairs are randomly chosen from the challenge-response database to form a challenge sequence ($C_J$) and a $L$-bit true key ($K_0$). Similar to the enrollment stage, the candidate optical PUF is illuminated by this challenge sequence successively and the scattered light is detected by the single-pixel detector, after that the detected signals are transformed into a $L$-bit unknown key ($K_?$) by comparing them with their median value. Next the normalized HD between $K_0$ and $K_?$ is calculated. If the normalized HD is below a preset threshold $x_c$, the candidate optical PUF is authenticated. In order to obtain a safer execution of authentication, all used challenge-response pairs will be discarded based on the principle of one-time pad.

Moreover, as previously discussed, parallel detection with multiple detectors can be used in the authentication protocol to improve the binary key-generation speed and efficiency, as well as to reduce the number of challenges required for each binary key, on the condition that multiple detectors are mounted far enough between each other.

V. CONCLUSION

In summary, we present a nonimaging-based scheme for authentication of optical PUFs executable at small speckle size with fingerprint physical information detected by a single-pixel detector. We theoretically and experimentally demonstrate that the intensity of the scattered light, with small-sized laser speckles fuzzy to the commonly used CCD or CMOS cameras, would fluctuate stochastically with the randomly encoded challenges. Binary keys obtained from the fluctuations are random, unique, unpredictable, and robust enough to be qualified for authentication applications. Authentication with these binary keys has been displayed and three methods have been illustrated to reduce the FRR and FAR dramatically, including increasing the key length, increasing the intensity of the scattered light and discarding challenges with low SNR, which greatly enhanced the security of the authentication since the critical security parameter FAR can be lowered even to the order of $10^{-28}$. Moreover, it is worth noting that our scheme is a universal method, which can be implemented with other types of single-pixel detector, in other spectral region, and even beyond the smallest speckle size observable by the commercial cameras.

Other detectors are also feasible for the proposed single-pixel detection scheme. Figure 8 shows the experimental results with the single-pixel photon detector replaced by a Si photodiode power meter (Thorlabs S130C) located reverse engineering of the optical PUF while simultaneously increasing the integration level of the application units, which are beneficial for the safety and compactness in real applications.

ACKNOWLEDGMENTS

We gratefully acknowledge the anonymous referee for helpful comments and constructive suggestions. This work is supported by Science Challenge Project (TZ2018003-3) and National Natural Science Foundation of China (Grants No. 61875178, No. 12175204, No. 61805218, and No. 12104423).

APPENDIX: UNIVERSALITY OF THE SINGLE-PIXEL-DETECTION-BASED AUTHENTICATION SCHEME

In this Appendix we demonstrate the universality of the proposed scheme, including implementations with other types of single-pixel detector, in other spectral region, and even beyond the smallest speckle size observable by the commercial cameras.

Other detectors are also feasible for the proposed single-pixel detection scheme. Figure 8 shows the experimental results with the single-pixel photon detector replaced by a Si photodiode power meter (Thorlabs S130C) located...
FIG. 9. (a) Intensity fluctuation of the scattered light detected by the power meter when illuminating the PUF with randomly modulated challenges. (b) Distribution of the detected intensities (blue bars) and the corresponding curve fitting with Eq. (2) (red line). (c) Distribution of intra-HD (in blue) and inter-HD I (in red). Laser wavelength: 1550 nm.

behind a pinhole (200 μm in diameter). The results are consistent with what is observed by the single-pixel photon detector.

The proposed single-pixel detection technique can also be utilized in other spectral regions. Figure 9 shows the experimental results with the He-Ne laser replaced by a telecom-band laser of 1550 nm and the single-pixel photon detector replaced by a Si photodiode-based infrared power meter (Thorlabs S132C) located behind a pinhole of diameter 200 μm, which are consistent with the results observed in the visible region of wavelength 632.8 nm.

To our knowledge, a commercial image sensor with the smallest pixel size is Samsung’s ISOCELL Slim GH1 whose pixel size is 0.7 μm. Using this image sensor, the smallest speckle of size 1.4 μm can be observed according to the Nyquist-Shannon sampling theorem, while for speckles smaller than 1.4 μm, fuzzy imaging will occur. We perform the experiment with a speckle size smaller than 1.4 μm, which shows that the proposed nonimaging scheme is still effective. Figure 10 presents the speckle pattern of size about 1.1 μm, inside which the speckle spot can not be observed clearly. This image is recorded by a CCD camera of pixel size 3.45 μm (Point Grey GS3-U3-51S5M-C), which is the smallest pixel size we can access (even though the pixel size of the camera on many commonly used mobile phone is about 1 μm, but the imaging lens integrated with the image sensor would affect the observation of such small speckles, so we do not use the mobile phone camera). The speckle size of 1.1 μm is obtained by extrapolation with the method introduced in Sec. II. Figure 11(a) plots the fluctuation of the fuzzy speckle response in Fig. 10, which is measured by a single-pixel photon detector (Thorlabs SPCM20A), and Fig. 11(b) displays its statistical distribution. Figure 11(c) shows the distribution of intra-HD and inter-HD I. Figure 11 demonstrates that this nonimaging authentication scheme is still effective for speckle patterns, which is fuzzy to the commercial image sensor of the highest resolution (i.e., of the smallest pixel size) at present.

FIG. 10. (a) Speckle pattern of speckle size about 1.1 μm recorded by a Point Grey CCD camera. (b) Magnification of the image in the dashed box in (a).

FIG. 11. (a) Number of photons detected by the single-pixel photon detector when illuminating the PUF with randomly modulated challenges. (b) Distribution of the detected photons (blue bars) and the corresponding curve fitting with Eq. (3) (red line). (c) Distribution of intra-HD (in blue) and inter-HD I (in red).
deformable-mirror spatial light modulator, Opt. Lett. 13, 10 (1988).

[40] S. Popoff, G. Lerosey, M. Fink, A. C. Boccola, and S. Gigan, Controlling light through optical disordered media: Transmission matrix approach, New J. Phys. 13, 123021 (2011).

[41] T. Kohlgraf-Owens and A. Dogariu, Finding the field transfer matrix of scattering media, Opt. Express 16, 13225 (2008).

[42] P. Lodahl, Quantum correlations induced by multiple scattering of quadrature squeezed light, Opt. Express 14, 6919 (2006).

[43] J. W. Goodman, Statistical Optics (John Wiley & Sons, New York, 2015).

[44] P. Wolf, G. Maret, E. Akkermans, and R. Maynard, Optical coherent backscattering by random media: An experimental study, J. Phys. 49, 63 (1988).

[45] A. Ishimaru, Wave Propagation and Scattering in Random Media Vol. 2 (Academic press, New York, 1978).

[46] M. Meretska, R. Uppu, G. Vissenberg, A. Lagendijk, W. Ijzerman, and W. L. Vos, Analytical modeling of light transport in scattering materials with strong absorption, Opt. Express 25, A906 (2017).

[47] J. R. Ott, N. A. Mortensen, and P. Lodahl, Quantum Interference and Entanglement Induced by Multiple Scattering of Light, Phys. Rev. Lett. 105, 090501 (2010).

[48] I. Hamarová, P. Šmíd, P. Horváth, and M. Hrabovský, Methods for determination of mean speckle size in simulated speckle pattern, Meas. Sci. Rev. 14, 177 (2014).

[49] D. Chicea, Speckle size, intensity and contrast measurement application in micron-size particle concentration assessment, Eur. Phys. J. Appl. Phys. 40, 305 (2007).

[50] T. Schürmann and P. Grassberger, Entropy estimation of symbol sequences, Chaos 6, 414 (1996).

[51] R. T. Cerbus and W. I. Goldburg, Information content of turbulence, Phys. Rev. E 88, 053012 (2013).

[52] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, National Institute of Standards and Technology (NIST) Special Publication 800-22, Rev. 1 (2010).

[53] H. Nili, G. C. Adam, B. Hoskins, M. Prezioso, J. Kim, M. R. Mahmoodi, F. M. Bayat, O. Kavehei, and D. B. Strukov, Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors, Nat. Electron. 1, 197 (2018).

[54] T. Tuncer, The implementation of chaos-based PUF designs in field programmable gate array, Nonlinear Dyn. 86, 975 (2016).

[55] S. Feng, C. Kane, P. A. Lee, and A. D. Stone, Correlations and Fluctuations of Coherent Wave Transmission through Disordered Media, Phys. Rev. Lett. 61, 834 (1988).

[56] S. Kay, Fundamentals of Statistical Signal Processing: Detection Theory (Prentice Hall, Englewood Cliffs, NJ, 1998).