Journal of Applied Physics | ARTICLE | scitation.org/journal/jap

Quantum advantage in biometric authentication with single photons

Cite as: J. Appl. Phys. **131**, 084401 (2022); doi: 10.1063/5.0080942
Submitted: 5 December 2021 · Accepted: 28 January 2022 ·
Published Online: 24 February 2022

View Online Export Citation CrossMark

Iannis K. Kominis[1,2,3,a)] and Michail Loulakis[4,5]

AFFILIATIONS

[1]Department of Physics, University of Crete, 71003 Heraklion, Greece
[2]Institute of Theoretical and Computational Physics, University of Crete, 71013 Heraklion, Greece
[3]Quantum Biometronics PC, 71409 Heraklion, Greece
[4]School of Applied Mathematical and Physical Sciences, National Technical University of Athens, 15780 Athens, Greece
[5]Institute of Applied and Computational Mathematics, FORTH, 71110 Heraklion, Greece

[a)]**Author to whom correspondence should be addressed:** ikominis@physics.uoc.gr

ABSTRACT

It was recently proposed to use the human visual system's ability to perform efficient photon counting in order to devise a new biometric methodology. The relevant biometric "fingerprint" is represented by the optical losses light suffers along several different paths from the cornea to the retina. The "fingerprint" is accessed by interrogating a subject on perceiving or not weak light flashes, containing few tens of photons, so that the subject's visual system works at the threshold of perception, at which regime optical losses play a significant role. Here, we show that if, instead of weak laser light pulses, we use quantum light sources, in particular, single-photon sources, we obtain a quantum advantage, which translates into a reduction of the interrogation time required to achieve the desired performance. Besides the particular application on biometrics, our work further demonstrates that quantum light sources can provide deeper insights when studying human vision.

Published under an exclusive license by AIP Publishing. https://doi.org/10.1063/5.0080942

I. INTRODUCTION

Secure biometric identification[1,2] has some analogies to secure transmission of information: in both cases, the potential for some impostor to maliciously intervene in the respective process must be avoided. Quantum cryptography[3,4] has served as a paradigm of the so-called "quantum advantage," i.e., the security of cryptographic key transmission is guaranteed by the laws of quantum physics. In contrast, classical means of information transmission are vulnerable to, e.g., eavesdropping.

In a similar fashion, we recently proposed[5] a biometric authentication scheme, which takes advantage of the human visual system's ability to perform photon counting. There, the laws of photon statistics and photodetection at the quantum level of a small number of photons are central for the workings of the scheme, providing for an uncompromising security against an impersonator. The relevant "fingerprint" is a physical property of the visual system, including the eyeball, retina, and brain. In other words, the biometric authentication process rests on the conscious perception of weak-intensity light, working at the very threshold of visual perception of a specially designed light stimulus. In particular, the "fingerprint" in this method is the optical loss suffered by light along its propagation from the cornea to the retina.

In our previous work,[5] the visual stimulus was supposed to originate from laser light. However, the number of photons in a pulse of laser light is known to fluctuate from pulse to pulse around a mean value, and these Poissonian fluctuations limit the performance of the authentication process as will be outlined later. Interestingly, quantum optical technology can now offer "quantum light" sources, in particular, single-photon sources, producing light with a much narrower distribution of the photon number. We will here show how such a quantum light source translates into a concrete quantum advantage of the authentication process, namely, a reduction in the interrogation time.

Besides its applied perspective, this work further signifies the promise of the emerging field of quantum vision,[6–11] one aspect of which is the use of quantum light sources to study human or

Published under an exclusive license by AIP Publishing

animal vision at a deeper level than was previously possible with classical light sources.

II. PRELIMINARIES

Our biometric authentication methodology was inspired by the early experiment of Hecht *et al.*,[12] eloquently described in modern terms by Bialek.[13] Hecht *et al.* unambiguously demonstrated that rod cells, the scotopic photoreceptors in our retina, are efficient photon detectors; moreover, they identified a threshold in the number of detected photons for visual perception to take place. We denote this threshold by K, which is found[12] to be $K \approx 6$. Parenthetically, a recent psychophysical experiment[14] performed along similar lines, but using a modern single-photon source for the stimulus light, found that $K \approx 1$. In any case, to our understanding, the precise value of K and its possible relation to the particular physiological condition of the subject is still an open problem.

In more detail, the three authors in Ref. 12 had their eyes illuminated by very weak-intensity light pulses, with the integrated photon number within each pulse being so small, that the visual perception became probabilistic, with the probability of seeing denoted by P_{see}. An expression for P_{see} can be found as follows. Denote by $\tilde{N}$ the mean number of photons within a light pulse of duration τ. Coherent light has Poissonian photon statistics, i.e., the probability to have exactly n photons within such a pulse is $\tilde{N}^n e^{-\tilde{N}}/n!$. Of course, the authors in Ref. 12 did not have lasers; however, it is known that for averaging times (in this case, the light pulse duration τ) longer than the correlation time of a classical light source the photon statistics are again Poissonian.[15]

However, when the mean number of photons per pulse incident on the eyeball is $\tilde{N}$, the actual mean number of photons per pulse *detected* by the retina's photoreceptors is reduced by a factor $0 < \alpha < 1$. This factor describes the optical losses suffered by light along its path from the cornea to the retina, as well as the probability of photodetection by the illuminated photoreceptors. Now, the probability that the number of photons detected by the illuminated patch of the retina is exactly n is given by $(\alpha\tilde{N})^n e^{-\alpha\tilde{N}}/n!$. If this number is higher than the detection threshold K, whatever its value, then the perception of "seeing" a spot of light will take place. Thus, the probability of seeing is

$$P_{\text{see}} = \sum_{n=K}^{\infty} \frac{(\alpha\tilde{N})^n e^{-\alpha\tilde{N}}}{n!}. \tag{1}$$

In Fig. 1, we plot examples of the dependence of the probability P_{see} on the mean number of photons per pulse incident on the cornea, $\tilde{N}$. In Fig. 1(a), we keep the threshold K constant at the value of $K = 6$ and change the loss factor α, whereas in Fig. 1(b) we keep α constant at the value $\alpha = 0.10$, and change K. Both dependences are rather obvious to interpret. It is important to note that the change of α [Fig. 1(a)] hardly changes the overall shape of the functional dependence of P_{see} vs $\tilde{N}$ and essentially shifts the figure along the x-axis. In contrast, the change of K qualitatively changes the shape of the dependence of P_{see} vs $\tilde{N}$. Now, although each one of the three authors in Ref. 12 produced a different dependence of P_{see} vs $\tilde{N}$, all three curves could be coalesced by such a translation along the x-axis, and all could be fit with a common value of $K \approx 6$. This is shown in Fig. 1(c).

The authors in Ref. 12 managed to make a remarkable case, despite the presence of a subjective observable, as is the optical loss parameter α, which changes among individuals and perplexes the analysis of individuals' responses to perceiving or not faint light pulses. The case is about two objective properties of the human visual system. The first has to do with the wiring of the photoreceptor cells to deeper neural layers communicating visual responses to the brain. This wiring determines the perception threshold K, which appears to be a common systemic property. The second is that retina's photoreceptors are efficient single-photon detectors. This follows from the fact that the experimentally inferred number of photons at the retina [see x-axis of Fig. 1(c)] is much smaller than the number of illuminated rod cells. It took several years until the quantum photo-detection properties of rod cells were unraveled with modern photonic and quantum-optical technology.[16–23]

III. QUANTUM BIOMETRICS

Our proposal on quantum biometrics[5] essentially turns the coin around: the variability of the parameter α among individuals was a nuisance for Hecht *et al.*, who were aiming at the single-photon-detection capability of rod cells. We now know this physiological capability is indeed the case. Instead, we would like to use the variability of the parameter α as a biometric quantifier. However, just one number is not enough as a biometric "fingerprint." Hence, the idea put forward in Ref. 5 is that the relevant "fingerprint" is a whole map of α values, the so-called α-map. This results from considering several paths of light toward the retina, illuminating the retina at several different spots. This point has to do with visual optics and will be further elaborated upon elsewhere.[24]

The crux of the matter is illustrated in Figs. 1(d)–1(f). Suppose we have an array of, e.g., nine laser beams, patterned in a 3×3 matrix [Fig. 1(d)]. Further suppose that these beams are all illuminated simultaneously; moreover, let us assume that the mean photon number per beam per pulse is very large, say, $\gg 100$ photons. In such a scenario, *every* subject (without any visual deficiency) will report seeing nine spots [Fig. 1(e)]. This is because, with certainty, everybody will perceive a pulse containing a large number of photons [far right in the curves of Figs. 1(a)–1(c), where $P_{\text{see}} \approx 1$]. However, as we reduce the mean photon number per laser beam per pulse, and move to the regime of the visual threshold described by the variable P_{see} in Figs. 1(a)–1(c), each individual will report different patterns of perception, as shown in Fig. 1(f). This difference in perception in the regime of the visual threshold is exactly what our biometric identification scheme takes advantage of.

To describe the methodology in more detail, we first note that as in all such psychophysical measurements with very weak light, the subject has to undergo dark adaptation, in order for scotopic rod vision to dominate the visual process. One prerequisite of our methodology is that the α-map of the subject that will need to be authenticated by the biometric device has been already measured and stored. This is like taking a subject's fingerprint and registering it in the relevant database. The process of registering the subject's

Published under an exclusive license by AIP Publishing

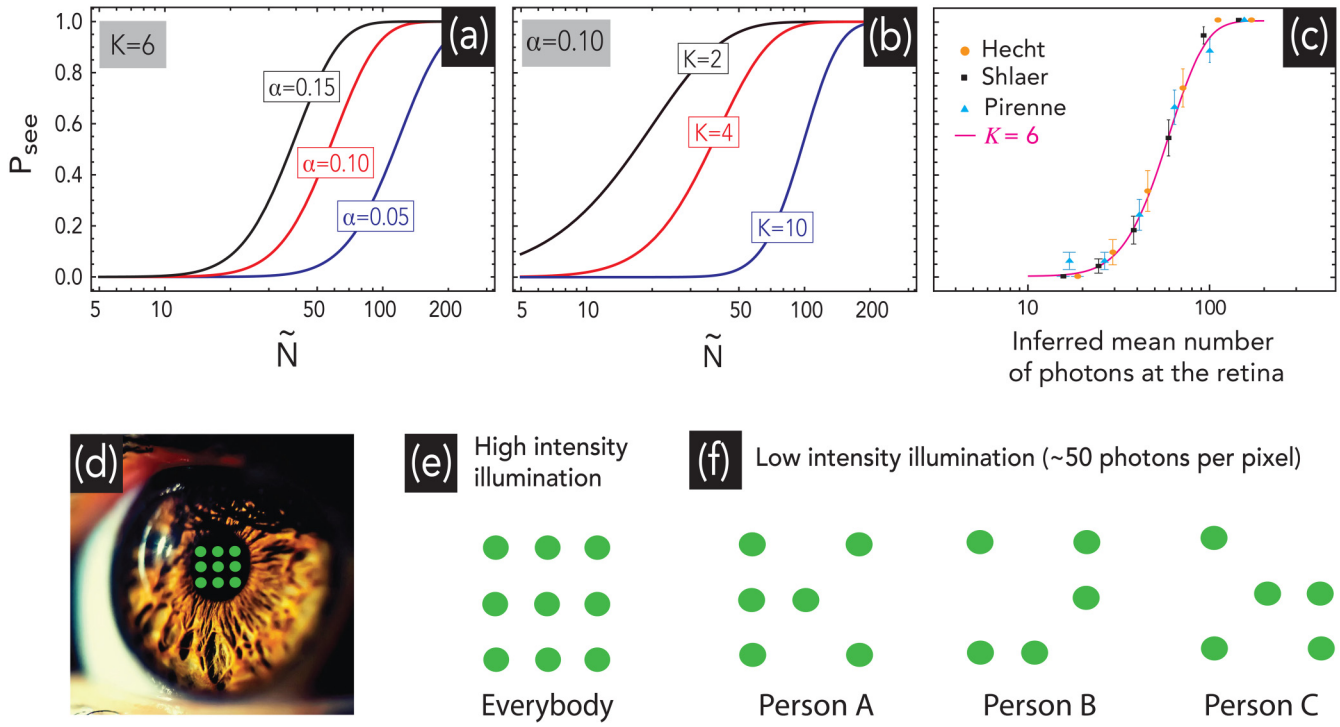

FIG. 1. Probability of seeing a light pulse having mean incident photon number per pulse $\tilde{N}$ vs $\tilde{N}$, as calculated from Eq. (1), for (a) various values of the optical loss parameter α, and constant perception threshold K, and (b) various values of K and constant α. (c) Experimental results of Ref. 12 for the probability of seeing by the three authors [figure reproduced with permission from Bialek, *Biophysics: Searching for Principles* (Princeton University Press, 2012). Copyright 2012 Princeton University Press]. In this figure, the x-axis is the inferred number of photons at the retina, i.e., the authors in Ref. 12 have shifted the curves of P_{see} along the x-axis using some factor α for each one of the three authors. This results in a "universal" response apparently having a common threshold K. For these authors, the difference in the α value among them was a nuisance for what they were trying to achieve, i.e., demonstrate the single-photon detection capability of rod cells. For us, this difference in α is taken advantage of to define our biometric quantifier. (d)–(f) Simplified presentation of the idea behind the biometric authentication using the photon counting capability of the human visual system. (d) A light stimulus source is supposed to provide for parallel laser beams patterned in an array, here shown as a 3×3 array. The laser beams propagate in parallel from the source to the eye, being incident on the cornea, all being simultaneously illuminated during a given pulse. If one could see the reflection of the laser beams off the cornea, one would see the image (d), where the pupil is shown to be illuminated by nine spots. (e) With each laser beam containing a large number of photons per pulse and further assuming that the human subject being illuminated is myopic, everybody would report seeing nine different spots patterned in such a 3×3 array. (f) However, if the number of photons per beam per pulse is reduced to the regime of 10–100 photons, the visual perception would be working close to its threshold. In such a case, the optical losses suffered by light along these nine different paths, different among paths for each individual, and different for a "geometrically similar" path among individuals will result in a different perception pattern for each subject.

"fingerprint" for the first time as well as the relevant ageing effects will be addressed elsewhere.[24]

When the subject wants to be authenticated, the biometric device must implement a measurement protocol, the result of which is either positive or negative. Thus, two central quantifiers of its performance are the false-negative and false-positive probability, denoted by p_{fn} and p_{fp}, respectively. The former is the probability that a subject truly claiming to be who he or she is, is *not* authenticated as such. The latter is the probability that an impostor falsely claiming to be somebody else is positively identified as that other person. Obviously, the longer the authentication process, the smaller these two probabilities should become. Hence, a third important performance quantifier is how much time is required to achieve a given desired value for p_{fn} and p_{fp}.

To proceed, we note that central to the authentication algorithms described in Ref. 5, as well as the one described here is that we choose to work with retinal spots associated with either too high or too low values of α. Let us call Alice the subject who appears and wishes to be positively authenticated. Eve will be an impostor maliciously claiming to be Alice. We will suppose that Eve is not aware of Alice's α-map. As a result, Eve does not know whether the device is illuminating a low-α or a high-α spot of Alice and, thus, cannot tune her responses accordingly. The spots being illuminated are randomly chosen by the device, and as far as Eve is concerned, they could be of any kind. Moreover, the device illuminates every spot, no matter of what kind, *with the same mean number of photons per pulse*. Thus, even if Eve is equipped with a perfect photon counter, she would just measure light pulses with a given mean number of photons. This measurement does not convey to her any useful information. Further, since she is not aware of Alice's α-map, even if Eve is equipped with a perfect position-sensitive photon detector, she still cannot extract any

Published under an exclusive license by AIP Publishing

useful information from any stimulus light patterns emitted by the biometric device. *Eve is forced to respond randomly to the device's interrogations on whether the subject does perceive or does not perceive the light flashes*. We will now quantify all of the above using a specific authentication protocol, which is a variant of the protocols given in Ref. 5. This variant and its modification when using a quantum light source are straightforward to understand.

A. Authentication protocol

We assume that the device simultaneously illuminates N different retinal spots, a random number H of which are high-α spots, the rest being low-α spots. The interrogated subject is then questioned on how many spots she perceived. We accept her answer, R, as correct, if $R = H$. There are two competing mechanisms that push Alice toward failure: the possibility that she does not see an illuminated high-α spot and the possibility that she does see an illuminated low-α spot.

B. Eve's strategy

Suppose Eve comes along claiming to be Alice and asking to be authenticated. We assume that Eve has access to the identification protocol and knows the distribution of the random variable H. Further suppose that she is equipped with perfect position-sensitive photon counters. She, thus, finds that N spots are being illuminated. Her answer on the device's interrogation about how many spots she perceived can be a random variable, call it X, which she chooses with some strategy. For sure, $X \perp\!\!\!\perp H$, that is, X is independent of H, since Eve does not know how many spots of which kind (high-α or low-α) are being illuminated. Thus, for her answer, she must use a random variable X independent of H, chosen so that the probability $\mathbb{P}[X = H]$ is maximized. But, it is

$$\mathbb{P}[X = H] = \sum_{m=0}^{N} \mathbb{P}[X = m, H = m] = \sum_{m=0}^{N} \mathbb{P}[X = m]\mathbb{P}[H = m]. \tag{2}$$

The second line follows from the independence of X from H and is a weighted average, which is maximized when the random variable X assumes those values m that maximize the probability $\mathbb{P}[H = m]$, that is, the modes of the distribution of H. For example, if H is unimodal, Eve's optimal response must be the mode of the distribution. In any case, since the range of values of H is $\{0, 1, \ldots, N\}$, there must be some $m \in \{0, 1, \ldots, N\}$ for which $\mathbb{P}[H = m] \geq 1/(N + 1)$. Thus,

$$\max_{X \perp\!\!\!\perp H} \mathbb{P}[X = H] \geq \frac{1}{N+1}. \tag{3}$$

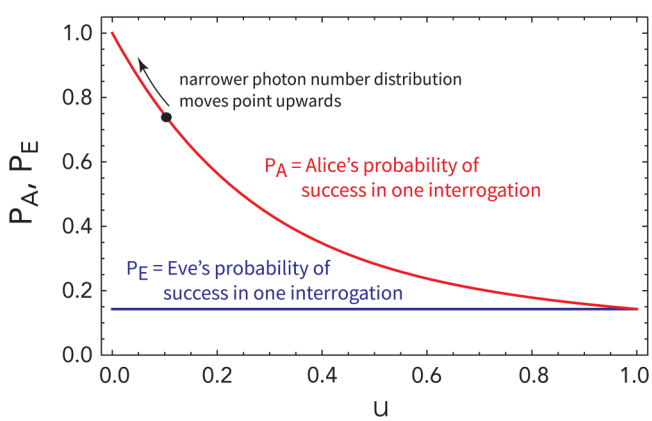

FIG. 2. Probability of Alice, P_A, and probability of Eve, P_E, correctly responding to one interrogation, consisting of illuminating a number of N spots in total (some of which are high-α and the rest low-α) and asking how many spots the subject perceived. The response counts as correct if the number of perceived spots equals the number of illuminated high-α spots. The probability P_A depends on $u = p_H + p_L$, which is the sum of the probability that Alice does not perceive an illuminated high-α spot, p_H, and the probability that she does perceives a low-α spot, p_L. The value of u depends on the photon statistics of the light; hence, narrower photon number distributions suppress u and, thus, provide for a quantum advantage. For this figure, $N = 6$.

C. Device's interrogation strategy

In view of the preceding analysis, the biometric device should choose the distribution of H to be as uninformative as possible, i.e., to be uniform on $\{0, 1, \ldots, N\}$. That is,

$$\mathbb{P}[H = k] = \frac{1}{N+1}, \qquad k = 0, 1, \ldots, N.$$

In such a case, regardless of her answer, Eve will have probability $\frac{1}{N+1}$ to answer correctly.

D. Positive authentication of Alice

We next consider Alice's probability of a successful answer, i.e., the probability $\mathbb{P}[Y = H]$, where Y stands for the number of spots Alice perceives. It is helpful to consider the number E_{fn} of high-α spots that Alice fails to perceive, as well as the number E_{fp} of low-α spots that Alice perceives. Clearly, $Y = (H - E_{fn}) + E_{fp}$, and Alice succeeds if the number of false-positive perceptions is equal to the number of false-negative perceptions. If Alice fails to perceive a stimulus on a high-α spot with probability p_H, and she perceives a stimulus on a low-α spot with probability p_L, then, conditionally on $H = k$, E_{fn} and E_{fp} are independent binomial random variables, with parameters (k, p_H) and $(N - k, p_L)$, respectively. The following Lemma is of interest on its own and does not have an immediate combinatorial interpretation. The proof is given in the Appendix.

Lemma 1 Suppose H is uniformly distributed on $[n] := \{0, 1, \ldots, n\}$ and, conditionally on $\{H = k\}$, the random variables Q and W are independent binomial with parameters

Published under an exclusive license by AIP Publishing

(k, p) and $(n-k, q)$. Then,

$$\mathbb{P}[Q = W] = \frac{1-(1-(p+q))^{n+1}}{(n+1)(p+q)}.$$

By setting $u = p_H + p_L$, a direct consequence of the Lemma is that Alice's probability of success reads

$$P_A = P_A(N, u) = \frac{1-(1-u)^{N+1}}{(N+1)u}. \tag{4}$$

For example, for $N = 6$ spots and $u = 0.1$, Alice succeeds in one interrogation with probability $P_A \simeq 0.745$, while an impostor, Eve, succeeds with probability $P_E = 1/7 \simeq 0.143$. The probabilities P_A and P_E are plotted in Fig. 2. As will become clear in the following, the value of $u = p_H + p_L$ for Alice depends on the photon statistics of the illuminating light source, so this is the point where the quantum advantage comes in.

E. Repeating the test to achieve a given p_{fp} and p_{fn}

In Fig. 3, we show how the authentication algorithm works. As mentioned above, the biometric device has stored Alice's α-map, so it can classify Alice's retinal spots into high-α spots, for which Alice has a high probability of seeing the light flash, and low-α spots, for which this probability is low. The device chooses the number N of spots it will illuminate (step 1). In the example of Fig. 3, it is $N = 5$. The specific value of N is the result of an optimization to be presented in the following.

We also define a success parameter S, which is initiated at the value $S = 0$ (step 2). Then, the device randomly selects a number $H \in \{0, 1, \ldots, N\}$ (step 3) and illuminates H spots of the type "high-α" and N–H spots of the type "low-α" (step 4). In the example of Fig. 3, it is $H = 2$. The subject is then (step 5) interrogated on how many bright spots she perceived. If her answer equals H, then we update the success parameter to $S = S + 1$, otherwise to $S = S - 1$. In the last step of the algorithm, S is compared with a positive upper value $S_+ > 0$ and with a negative lower value $S_- < 0$. If $S = S_+$, we stop the interrogation process, authenticating the subject as Alice. If $S = S_-$, then we stop the process with a negative authentication, i.e., the subject is not Alice. Otherwise, we return to step 3 of the algorithm.

The choice of S_+ and S_- depends on the desired values of p_{fp} and p_{fn}, as follows. Both Alice and Eve perform a random walk in S-space with unit step and probabilities P_A and P_E, respectively, for a positive step, and $1 - P_A$ and $1 - P_E$, respectively, for a negative step. If by $\tau_{S_\pm} = \inf\{k \geq 0 : S_k = S_\pm\}$ we denote the interrogation round in which S first reaches $S_\pm$, then[31] the probability that Eve's success parameter reaches the value S_+ and, thus, Eve is falsely identified as Alice is

$$\mathbb{P}_E[\tau_{S_+} < \tau_{S_-}] = \frac{1-N^{S_-}}{N^{S_+} - N^{S_-}} \lessapprox N^{-S_+}. \tag{5}$$

Thus, Eq. (5) is the probability that Eve will reach the value S_+ expected for Alice's authentication before reaching the value S_- expected for Eve's non-authentication. To ensure that this probability is smaller than the specified tolerance p_{fp}, we may choose $S_+ = S_+(N)$ to be

$$S_+(N) = \left\lceil -\frac{\log p_{fp}}{\log N} \right\rceil, \tag{6}$$

where $\lceil x \rceil$ stands for the smallest integer greater than or equal $x \in \mathbb{R}$.

Similarly, the probability that Alice's S parameter drifts to the low value S_- and, thus, Alice is falsely not authenticated, is equal to

$$\mathbb{P}_A[\tau_{S_-} < \tau_{S_+}] = \frac{1-\left(\frac{1-P_A}{P_A}\right)^{S_+}}{\left(\frac{1-P_A}{P_A}\right)^{S_-} - \left(\frac{1-P_A}{P_A}\right)^{S_+}} \lessapprox \left(\frac{P_A}{1-P_A}\right)^{S_-}. \tag{7}$$

To ensure that this probability is smaller than the specified tolerance p_{fn}, we may choose

$$S_- = S_-(N) = \left\lfloor \frac{\log p_{fn}}{\log\left(\frac{P_A}{1-P_A}\right)} \right\rfloor, \tag{8}$$

where $\lfloor x \rfloor$ stands for the greatest integer not exceeding $x \in \mathbb{R}$.

IV. QUANTUM ADVANTAGE USING QUANTUM LIGHT

We are now in position to explore the quantum advantage brought about by quantum light, in particular, a single-photon source. Since the temporal summation window[25] of the visual system is on the order of $\tau_{ts} \approx 400$ms, we can use a single-photon source, for example, a heralded single-photon source,[26–29] to produce a maximum of $\tilde{N} \sim 200$ photons within a time interval τ_{ts}, i.e., we need a production rate of at most 1 kHz, which is readily feasible. In the ideal case, the probability distribution of the number of photons incident on the cornea will be $p(n) = \delta_{n,\tilde{N}}$.

It is known, however, that optical losses degrade the sub-Poissonian statistics of quantum light. Hence, if a pulse of light containing exactly $\tilde{N}$ photons propagates inside the lossy material of the eye, the statistics of the number of detected photons will not be a spiked distribution like $p(n)$, but a broader distribution. Since the optical losses quantified by the parameter α are not insignificant, the distribution of the detected photon number is not very far from the case of coherent light discussed previously. Yet, we will show that single photons do enhance performance, which demonstrates that quantum light sources can indeed be useful in addressing human vision.

The photon number after propagation through the lossy material is given for a quantum or a coherent light pulse, respectively, by

$$P_q = \sum_{i=1}^{\tilde{N}} W_i \quad \text{and} \quad \mathrm{P_c} = \sum_{\mathrm{i}=1}^{\mathrm{M}} \mathrm{W_i}. \tag{9}$$

In the preceding equation, M is the Poisson random variable with mean $\tilde{N}$, and, for an optical loss parameter α, W_i are Bernoulli(α)

Published under an exclusive license by AIP Publishing

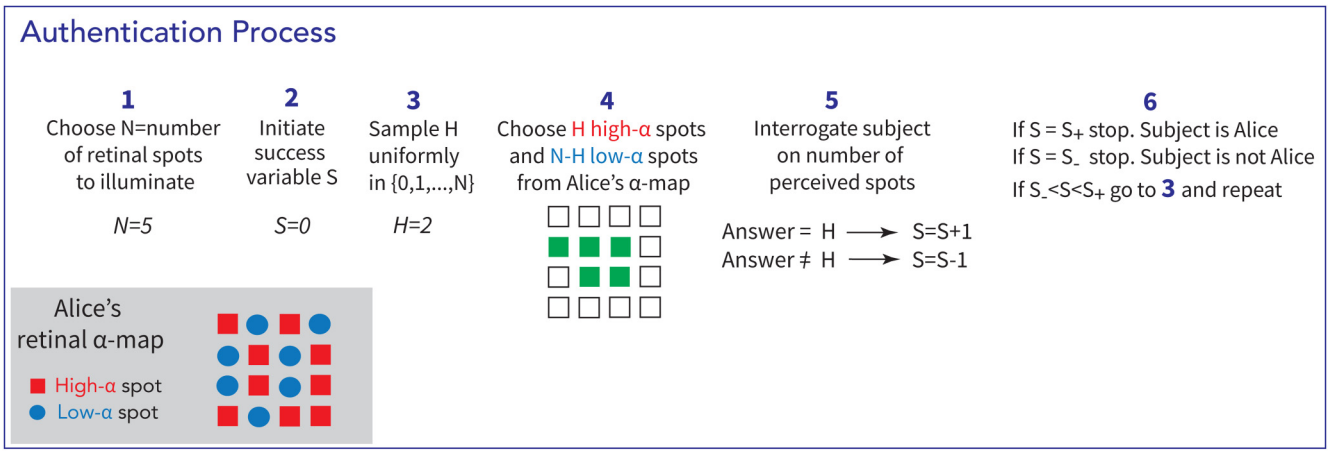

FIG. 3. Authentication algorithm. We suppose the biometric device has already measured and stored Alice's α-map and has classified her retinal spots (in this example, in a grid of 5×5 spots) into high-α and low-α spots, shown in the inset as red squares and blue circles, respectively. A subject approaches the device and claims to be Alice. The first step of the authentication algorithm is to choose a number N of spots to illuminate, in this example $N = 5$. Then, we initiate the success variable S to the value $S = 0$. In the third step, we uniformly sample $H \in \{0, 1, \ldots, N\}$. In step 4, we choose H high-α and $N - H$ low-α spots to illuminate. In this example, $H = 2$, which means that the device will illuminate two high-α spots and three low-α spots, as in step 4. In step 5, the subject is interrogated on the number of spots she perceived, and if her answer is H, the success variable S is updated by $S = S + 1$, otherwise $S = S - 1$. In the final step 6, the device compares S with S_- and S_+, which are defined in the text and are derived from the required performance on p_{fp} and p_{fn}. As long as $S_- < S < S_+$, we repeat the algorithm going back to step 3. In case S reaches S_+ the algorithm stops and the subject is authenticated as Alice, whereas if S reaches S_- the subject is not authenticated as Alice.

random variables that indicate whether the ith photon of the pulse was detected or not. In particular, the distribution of P_q is binomial with parameters $(\tilde{N}, \alpha)$, i.e.,

$$p_q(n; \alpha) = \frac{\tilde{N}!}{n!(\tilde{N} - n)!} \alpha^n (1 - \alpha)^{\tilde{N} - n}, \qquad n = 0, 1, \ldots, \tilde{N}, \quad (10)$$

whereas the distribution of P_c is Poisson with mean $\alpha\tilde{N}$, i.e.,

$$p_c(n; \alpha) = e^{-\alpha\tilde{N}} \frac{(\alpha\tilde{N})^n}{n!}, \qquad n = 0, 1, \ldots. \quad (11)$$

It follows from Theorem 8.A.13 (b) in Ref. 30 that P_c dominates P_q in the *convex order*, i.e., for every convex function ϕ on $\mathbb{Z}_+$,

$$\mathbb{E}[\phi(P_q)] \leq \mathbb{E}[\phi(P_c)]. \quad (12)$$

Comparison in the convex order essentially compares the concentration around a common mean; thus, (12) indicates that P_c has a broader distribution than P_q. For instance, taking $\phi(x) = (x - \alpha\tilde{N})^2$, we see that P_c has larger variance than P_q. Indeed, the variance of the number of photons detected at the retina is $V(P_c) = \alpha\tilde{N}$ with coherent light, whereas the corresponding variance with quantum light is $V(P_q) = \alpha(1 - \alpha)\tilde{N}$. In Fig. 4(a), we show an example of the slight difference of the two distributions, Eqs. (10) and (11), for $\alpha = 0.16$ and $\tilde{N} = 60$ photons.

Now, the probability that Alice fails to perceive an illuminated high-α spot is

$$p_H(\tilde{N}) = \sum_{n=0}^{K-1} p(n; \alpha_H), \quad (13)$$

whereas the probability that Alice does perceive an illuminated low-α spot is

$$p_L(\tilde{N}) = 1 - \sum_{n=0}^{K-1} p(n; \alpha_L). \quad (14)$$

In these expressions, the probability mass function $p(n; \alpha)$ is equal to either $p_q(n; \alpha)$ of Eq. (10) for quantum light or to $p_c(n; \alpha)$ of Eq. (11) for laser light. The parameter $u = p_H(\tilde{N}) + p_L(\tilde{N})$ enters Eq. (4), giving the probability that Alice succeeds in one particular interrogation. An example of the dependence of the parameter u on the incident mean photon number $\tilde{N}$ is shown in Fig. 4(b). It is seen that u is minimized at $\tilde{N} \simeq 69.32$ for laser light and $\tilde{N} = 68$ for single photons, the minimum being $u_c = 0.0983$ and $u_q = 0.0838$, respectively. (Note that for a coherent state relevant to laser light $\tilde{N}$ is a continuous variable.)

A. Number of interrogations

Having found Alice's parameter u for a given set of values α_H and α_L, we can use Eq. (4) to determine the mean number, T_A, of interrogations required for Alice's authentication, and choose the number of illuminated spots, N, to minimize T_A. Indeed, by

Published under an exclusive license by AIP Publishing

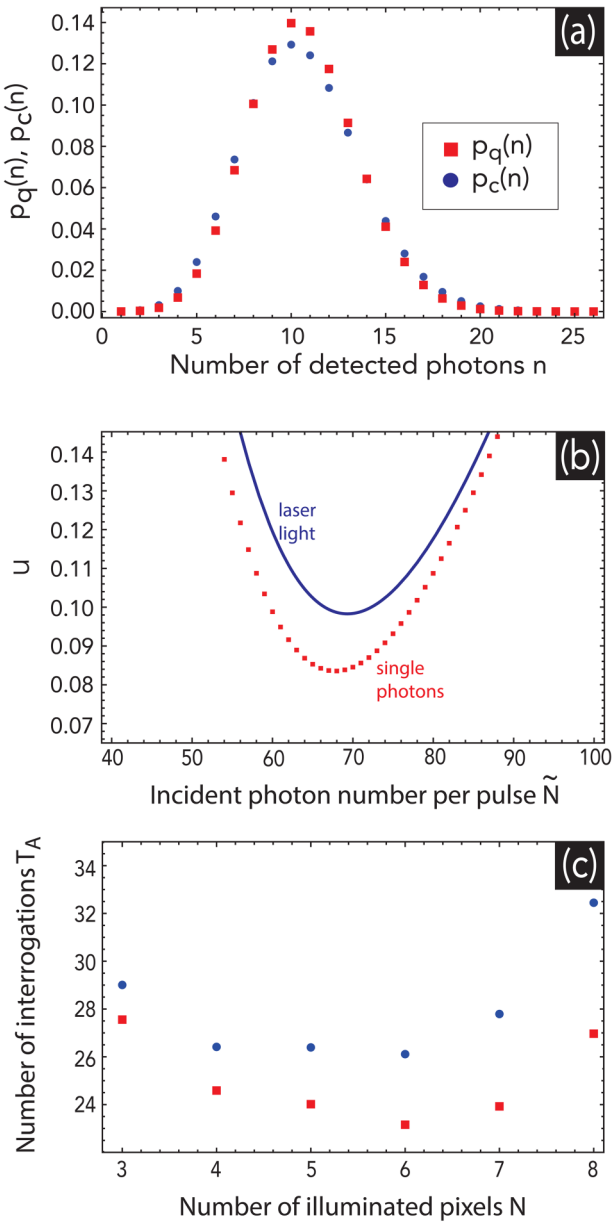

FIG. 4. Quantum advantage with single photons. (a) Example of the distribution of n, the photon number after transmission through the lossy material of loss parameter α, which here is $\alpha = 0.16$, and for an incident photon number $\tilde{N} = 60$. For the incident light being coherent laser light, the distribution is $p_c(n)$, whereas for a pulse of 60 single photons incident on the eye the distribution is $p_q(n)$. The distribution $p_q(n)$ is slightly narrower than $p_c(n)$. (b) Example of the dependence of $u = p_H + p_L$ on the mean number of incident photons per pulse, $\tilde{N}$, for laser light and single photons. The minimum in each case determines the optimal mean photon number $\tilde{N}$. Here, $\alpha_H = 0.16$ and $\alpha_L = 0.04$. (c) Number of interrogations T_A vs number of illuminated pixels N, for laser light and single photons. The minimum in each case determines the optimal number N of pixels that should be illuminated and the corresponding optimal number of interrogations T_A. The quantum advantage is a 11.4% reduction in T_A. Blue circles refer to laser light and red squares to single photons.

Theorem 1.3.5 in Ref. 31, we find

$$T_A = \frac{S_+}{2P_A - 1} - \frac{S_+ - S_-}{2P_A - 1}\mathbb{P}_A[\tau_{S_-} < \tau_{S_+}] \lessapprox \frac{S_+}{2P_A - 1}, \tag{15}$$

where the second term in the exact expression for T_A was neglected as it is proportional to $p_{fn} \ll 1$, and where $S_+ = S_+(N)$ is given by (6), $S_- = S_-(N)$ is given by (8), and $P_A = P_A(N, u)$ is given by (4). In Fig. 4(c), we plot T_A vs the number of illuminated retinal spots (pixels) N for the two cases we consider, i.e., laser light and single photons. It is seen that for laser light the optimal number of expected interrogations is $T_A \simeq 26.1$, with the optimal number of spots being $N = 6$. For single photons, we find an optimal of approximately 23.1 expected interrogations with $N = 6$ illuminated spots, i.e., we gain about 11.4% in total interrogation time. Finally, if we consider the photon number as a resource, the fact that the optimal photon number per pulse for quantum light ($\tilde{N} = 68$) is somewhat smaller than the corresponding number for laser light ($\tilde{N} = 69.32$) pushes the total advantage to 13.1%.

V. DISCUSSION

We have here presented an intuitive biometric authentication process using the human visual system's ability to perform photon counting. The process rests on the perception of a number of illuminated spots on the retina. The performance of the authentication process in terms of false positive and false negative probability, as well as the interrogation time required to realize those two probabilities, is determined by the photon statistics of the stimulus light. We have shown that a single-photon source provides an advantage, even though the optical losses, which form the biometric fingerprint, degrade the sub-Poissonian statistics of the quantum stimulus light. Two comments are to be made. First, one might claim that the quantum advantage is small. However, a significantly larger quantum advantage cannot be excluded. This is because it is not straightforward to find the ultimate quantum limit of the general methodology, independent of the specific authentication strategy. Indeed, since the visual perception involves a number of nonlinearities, one might expect to be able to enhance the small difference in photon statistics between laser light and quantum light (at the photon detection level discussed previously) by designing another interrogation strategy. In the same context, one might argue that despite the quantum advantage shown here, the number of required interrogations is anyhow large. This is the reason we previously[5] devised an authentication strategy based on pattern recognition. This strategy led to a much faster authentication time with the same performance metrics. However, this strategy depends on further assumptions on the workings of visual perception and pattern recognition. In contrast, with the simple strategy considered herein, we aimed at a straightforward to understand, and analytically tractable demonstration of the promise of quantum light sources for studying the human visual system, in general, and our biometric authentication methodology, in particular.

ACKNOWLEDGMENTS

This work has been co-financed by the European Union and Greek national funds through the Operational Program

Published under an exclusive license by AIP Publishing

Competitiveness, Entrepreneurship and Innovation, under the call "RESEARCH-CREATE- INNOVATE," with project title "Photonic analysis of the retina's biometric photo-absorption" (Project Code T1EDK-04921).

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts of interest to disclose.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

APPENDIX: PROOF OF LEMMA 1

The proof of the Lemma is as follows:

$$\begin{aligned}\mathbb{P}[U=V] &= \frac{1}{n+1}\sum_{k=0}^{n}\mathbb{P}[U=V|\ H=k]\\ &= \frac{1}{n+1}\sum_{k=0}^{n}\sum_{j=0}^{k}\mathbb{P}[U=j|\ H=k]\ \mathbb{P}[V=j|\ H=k]\\ &= \frac{1}{n+1}\sum_{k=0}^{n}\sum_{j=0}^{k}\binom{k}{j}\binom{n-k}{j}p^j(1-p)^{k-j}q^j(1-q)^{n-k-j}.\end{aligned} \tag{A1}$$

For a set $A \subset [n]$ of odd cardinality and median k, and for $x \in [n]$, we define

$$c(x, A) = \begin{cases} p, & \text{if x} \in \text{A and x} < \text{k} \\ 1-p, & \text{if x} \notin \text{A and x} < \text{k} \\ 1, & \text{if x} = \text{k} \\ q, & \text{if x} \in \text{A and x} > \text{k} \\ 1-q, & \text{if x} \notin \text{A and x} > \text{k} \end{cases} \tag{A2}$$

and $c(A) = \prod_{x=0}^{n} c(x, A)$. It is immediate that if $|A| = 2j+1$, then $c(A) = p^j(1-p)^{k-j}q^j(1-q)^{n-k-j}$. On the other hand, there are precisely $\binom{k}{j}\binom{n-k}{j}$ sets $A \subset [n]$ with median k and cardinality $|A| = 2j+1$, since there are $\binom{k}{j}$ ways to choose the j elements of A in $\{0, \ldots, k-1\}$ and $\binom{n-k}{j}$ ways to choose the j elements of A in $\{k+1, \ldots, n\}$. Hence, with $\gamma_n := \sum_{\substack{A\subset[n]\\|A|\text{odd}}} c(A)$, it is

$$\gamma_n = \sum_{k=0}^{n}\sum_{j=0}^{k}\binom{k}{j}\binom{n-k}{j}p^j(1-p)^{k-j}q^j(1-q)^{n-k-j}. \tag{A3}$$

We can straightforwardly compute

$$\gamma_0 = 1 \quad \text{and} \quad \gamma_1 = 1 - \text{p} + 1 - \text{q} = 2 - (\text{p} + \text{q}). \tag{A4}$$

For $n \geq 2$, we have

$$\begin{aligned}\gamma_n &= \sum_{\substack{\{0,n\}\subset A\subset[n]\\|A|\text{odd}}} c(A) + \sum_{\substack{A\subset[n],\{0,n\}\cap A^c\neq\emptyset\\|A|\text{odd}}} c(A)\\ &= \sum_{\substack{\{0,n\}\subset A\subset[n]\\|A|\text{odd}}} c(A) + \sum_{\substack{A\subset[n],\ 0\notin A\\|A|\text{odd}}} c(A)\\ &\quad + \sum_{\substack{A\subset[n],\ n\notin A\\|A|\text{odd}}} c(A) - \sum_{\substack{A\subset[n],\ 0,n\notin A\\|A|\text{odd}}} c(A).\end{aligned} \tag{A5}$$

If $0, n \in A$ then

$$c(A) = pq\prod_{x=1}^{n-1} c(x, A) = pq\prod_{x=0}^{n-2} c(x, \tilde{A}) = pq\ c(\tilde{A}),$$

where $\tilde{A} = A \setminus \{0, n\} - 1 \subset [n-2]$. Hence,

$$\sum_{\substack{\{0,n\}\subset A\subset[n]\\|A|\text{odd}}} c(A) = pq\sum_{\substack{\tilde{A}\subset[n-2]\\|\tilde{A}|\text{odd}}} c(\tilde{A}) = pq\ \gamma_{n-2}.$$

Likewise,

$$\begin{aligned}\sum_{\substack{\{0,n\}\subset A^c\subset[n]\\|A|\text{odd}}} c(A) &= (1-p)(1-q)\sum_{\substack{\tilde{A}\subset[n-2]\\|\tilde{A}|\text{odd}}} c(\tilde{A})\\ &= (1-p)(1-q)\gamma_{n-2}\end{aligned} \tag{A6}$$

and

$$\sum_{\substack{A\subset[n],\ 0\notin A\\|A|\text{odd}}} c(A) = (1-p)\ \gamma_{n-1}, \qquad \sum_{\substack{A\subset[n],\ n\notin A\\|A|\text{odd}}} c(A) = (1-q)\ \gamma_{n-1}.$$

We may now substitute the preceding relations in (A5) to get the recursive equation

$$\gamma_n = (2-p-q)\gamma_{n-1} + (p+q-1)\gamma_{n-2}, \qquad \text{for all n} \geq 2.$$

In view of the initial condition (A4), the assertion of the Lemma can now be proved inductively, or simply by noting that γ_n depends on p, q only through $p+q$ and setting $q \leftarrow 0,\ p \leftarrow p+q$ in Eq. (A1).

REFERENCES

[1] J. A. Unar, W. C. Seng, and A. Abbasi, Pattern Recognit. **47**, 2673 (2014).
[2] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, Sensors **21**, 6163 (2021).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] S. Pirandola *et al.*, Adv. Opt. Phot. **12**, 1012 (2019).
[5] M. Loulakis, G. Blatsios, C. S. Vrettou, and I. K. Kominis, Phys. Rev. Appl. **8**, 044012 (2017).
[6] P. Sekatski, N. Brunner, C. Branciard, N. Gisin, and C. Simon, Phys. Rev. Lett. **103**, 113601 (2009).
[7] N. Brunner, C. Branciard, and N. Gisin, Phys. Rev. A **78**, 052110 (2008).
[8] F. Lucas and K. Hornberger, Phys. Rev. Lett. **113**, 058301 (2014).
[9] R. Pizzi, R. Wang, and D. Rossetti, PLoS One **11**, e0147464 (2016).

Published under an exclusive license by AIP Publishing

[10]A. Dodel, A. Mayinda, E. Oudot, A. Martin, P. Sekatski, J.-D. Bancal, and N. Sangouard, Quantum **1**, 7 (2017).
[11]A. Pedram, Ö. E. Müstecaplıoğlu, and I. K. Kominis, arXiv:2111.03285.
[12]S. Hecht, S. Shlaer, and M. H. Pirenne, J. Gen. Phys. **25**, 819 (1942).
[13]W. Bialek, *Biophysics: Searching for Principles* (Princeton University Press, 2012).
[14]J. N. Tinsley, M. I. Molodtsov, R. Prevedel, D. Wartmann, J. Espigulé-Pons, M. Lauwers, and A. Vaziri, Nat. Commun. **7**, 12172 (2016).
[15]M. Fox, *Quantum Optics* (Oxford University Press, 2006).
[16]D. A. Baylor, T. D. Lamb, and K.-W. Yau, J. Physiol. **288**, 613 (1979).
[17]F. Rieke and D. A. Baylor, Biophys. J. **71**, 2553 (1996).
[18]F. Rieke and D. A. Baylor, Biophys. J. **75**, 1836 (1998).
[19]F. Rieke and D. A. Baylor, Rev. Mod. Phys. **70**, 1027 (1998).
[20]N. Sim, D. Bessarab, C. M. Jones, and L. A. Krivitsky, Biomed. Opt. Express **2**, 2926 (2011).
[21]N. Sim, M. F. Cheng, D. Bessarab, C. M. Jones, and L. A. Krivitsky, Phys. Rev. Lett. **109**, 113601 (2012).
[22]N. M. Phan, M. F. Cheng, D. A. Bessarab, and L. A. Krivitsky, Phys. Rev. Lett. **112**, 213601 (2014).
[23]P. C. Nelson, Phys. Biol. **13**, 025001 (2016).
[24]I. K. Kominis, M. Loulakis, and Ö. E. Müstecaplıoğlu, in *Recent Advances in Biometrics*, edited by M. Sarfraz (IntechOpen, 2022).
[25]R. Holmes, M. Victora, R. F. Wang, and P. G. Kwiat, Vis. Res. **140**, 33 (2017).
[26]M. Oxborrow and A. G. Sinclair, Contemp. Phys. **46**, 173 (2005).
[27]G. S. Buller and R. J. Collins, Meas. Sci. Technol. **21**, 012002 (2010).
[28]M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Rev. Sci. Instrum. **82**, 071101 (2011).
[29]E. Meyer-Scott, C. Silberhorn, and A. Migdall, Rev. Sci. Instrum. **91**, 041101 (2020).
[30]M. Shaked and J. G. Shanthikumar, *Stochastic Orders* (Springer, New York, 2007).
[31]J. R. Norris, *Markov Chains* (Cambridge University Press, 1998).

Published under an exclusive license by AIP Publishing