Open access • Journal Article • DOI:10.1364/OL.36.000022

Information authentication using photon-counting double-random-phase encrypted images — Source link

Elisabet Pérez-Cabré, Myungjin Cho, Bahram Javidi

Institutions: Polytechnic University of Catalonia, University of Connecticut

Published on: 01 Jan 2011 - Optics Letters (The Optical Society)

Topics: On-the-fly encryption, Encryption, Filesystem-level encryption, Multiple encryption and Disk encryption

Information authentication using photon-counting double-random-phase encrypted images

Elisabet Pérez-Cabré,[1,*] Myungjin Cho,[2] and Bahram Javidi[2,3]

[1]*Departament Òptica i Optometria, Universitat Politècnica Catalunya, Violinista Vellsolà 37, 08222 Terrassa, Spain*

[2]*Electrical & Computer Engineering Department, University of Connecticut, 371 Fairfield Road Unit 2157 Storrs, Connecticut 06269, USA*

[3]*e-mail: bahram@engr.uconn.edu*

**Corresponding author: elisabet.perez@upc.edu*

Received August 6, 2010; revised October 20, 2010; accepted November 19, 2010; posted November 22, 2010 (Doc. ID 132878); published December 17, 2010

Photon-counting imaging is integrated with optical encryption for information authentication. An image is double-random-phase encrypted, and a photon-limited encrypted image is obtained. The photon-counting encrypted image is generated with few photons and appears sparse; however, we show that it has sufficient information for decryption and authentication. The decrypted image cannot be easily visualized so that an additional layer of information protection is achieved. The authentication is carried out by recognition algorithms. This approach may make the verification process more robust against attacks. To the best of our knowledge, this is the first report on integrating photon-counting imaging and encryption for authentication.

OCIS codes: 060.4785, 100.4998, 030.5260, 070.5010, 070.4340, 100.4992.

Optical encryption techniques have been widely investigated [1–7]. A number of algorithms exist to produce a noisylike distribution that contains the information of a primary image [1–7]. These techniques have been shown to be useful to protect information that needs to be kept secret. One of the most widespread techniques, the double-random-phase encryption (DRPE) [2], has been recently shown to be vulnerable to certain attacks when the keys for decryption are used repeatedly without being updated [8,9]. To overcome this difficulty, we propose to integrate the photon-counting imaging technique with optical encryption. Photon-counting techniques have been applied in many fields [10–12]. In photon-counting imaging systems, images can have a limited number of photons by controlling the expected number of incident photons [12].

In this Letter, we propose to use photon-counting imaging to obtain a photon-limited version of the encrypted distribution. As a consequence, a sparse representation of the encrypted function is used for decryption. The sparse encrypted distribution produces a decoded image that cannot be easily recognized by intruders. The decrypted image is intended not for direct visualization of the primary image but for verification of the information by means of optical correlation. This procedure may provide an additional layer of protection and may make the verification process more robust against attacks.

We briefly detail the DRPE [2]. Let $f(x)$ be the primary image in one-dimensional notation for simplicity [Fig. 1(a)]. Let $n(x)$ and $b(\mu)$ be two random noises uniformly distributed over $[0, 1]$. The coordinates (x) and (μ) correspond to the spatial and the frequency domain, respectively. First, image $f(x)$ is multiplied by the phase mask $\exp[i2\pi n(x)]$. The resulting product is then convolved by function $h(x)$, for which the Fourier transform is $\mathrm{FT}\{h(x)\} = \exp[i2\pi b(\mu)]$. The final encrypted distribution, $\psi(x)$, is a complex-valued function defined by

$$\psi(x) = \{f(x)\exp[i2\pi n(x)]\} * h(x), \tag{1}$$

where $*$ denotes convolution. The complex-amplitude encrypted image $\psi(x)$ must be represented with both amplitude, $|\psi(x)|$, and phase information, $\phi_\psi(x)$, so it can be also written as $\psi(x) = |\psi(x)|\exp[i\phi_\psi(x)]$. In general, the encrypted function has a noisy appearance that does not reveal its content, as can be seen in Fig. 1(b), which shows the amplitude distribution of the encrypted signal obtained from Fig. 1(a).

To generate a photon-limited encrypted image, $\psi_{\mathrm{ph}}(x)$, by controlling the number of counts in the entire scene, N_p, a photon-counting imaging approach is used. The probability of counting l_j photons at pixel j can be shown to be Poisson distributed [12,13]:

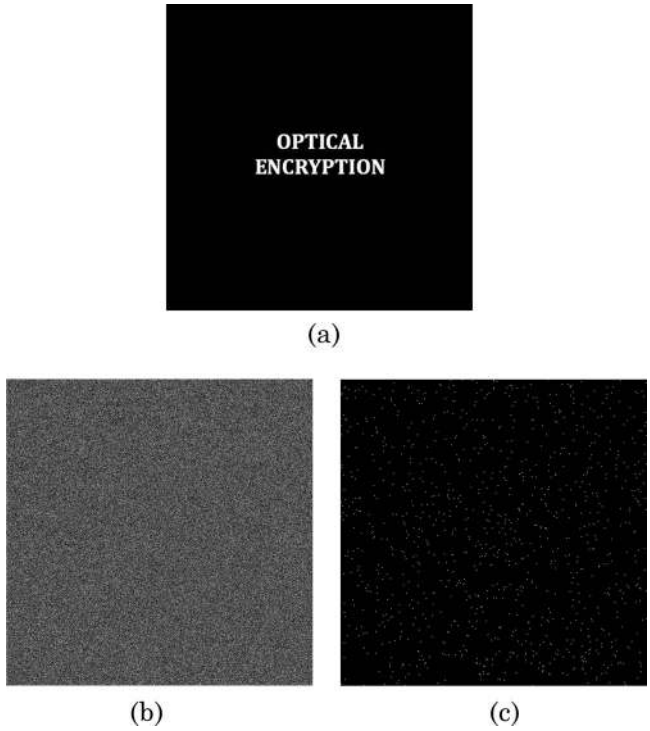

Fig. 1. (a) Image $f(x)$; (b) function $|\psi(x)|$; (c) function $|\psi_{\mathrm{ph}}(x)|$ with $N_p = 10^3$.

$$P_d(l_j;\lambda_j)=\frac{[\lambda_j]^{l_j}e^{-\lambda_j}}{l_j!},\qquad l_j=0,1,2,\ldots, \tag{2}$$

where l_j is the number of photons detected at pixel j and the Poisson parameter, λ_j, is given by $\lambda_j=N_p x_j$ with x_j being the normalized irradiance at pixel j, such that $\sum_{j=1}^{M} x_j=1$, and M equals the total number of pixels in the scene.

The photon-counting imaging approach is applied to the complex-valued encrypted distribution $\psi(x)$. The photon-limited amplitude data, $|\psi_{\mathrm{ph}}(x)|$, is generated by applying the aforementioned procedure to the normalized amplitude distribution, $|\psi(x_j)|/\sum_{i=1}^{M}|\psi(x_i)|$. The pixels that receive at least one photon count are considered in the photon-limited encrypted function, $\psi_{\mathrm{ph}}(x)$. Only these pixels contain information about the amplitude and the phase for decryption. Figure 1(c) shows the magnitude of the photon-limited encrypted function, $\psi_{\mathrm{ph}}(x)$, corresponding to Fig. 1(b) when the total number of counts is set to be $N_p=10^3$ and the maximum number of photons per pixel is 2.

According to the DRPE method [2] described by Eq. (1), to decrypt the information, the encrypted function $\psi_{\mathrm{ph}}(x)$ is first Fourier transformed and multiplied by the decryption key, $\exp[-i2\pi b(\mu)]$. Thus, function $f_{\mathrm{ph}}(x)\exp[i2\pi n(x)]$ is obtained. Provided that the original image, $f(x)$, is a real and positive function, an intensity-sensitive device such as a CCD camera will retrieve the photon-limited decrypted image $f_{\mathrm{ph}}(x)$. Figure 2(a) shows the decrypted image obtained from the sparse encrypted distribution of Fig. 1(c). The text contained in the primary image [Fig. 1(a)] is hardly recognized in the noisy background of the decoded image [Fig. 2(a)].

To authenticate the retrieved signal $f_{\mathrm{ph}}(x)$, we compare it with the original image, $f(x)$, used as the reference, by nonlinear correlation [14]. However, a number of other recognition approaches may be used [15–17]. The signals to be compared are Fourier transformed, nonlinearly modified, and multiplied in the frequency domain. By inverse Fourier transforming this product, the nonlinear correlation, $c(x)$, between both signals is obtained [14]:

$$c(x)=\mathrm{IFT}\{|F_{\mathrm{ph}}(\mu)F(\mu)|^k\exp[i(\phi_{F_{\mathrm{ph}}}(\mu)-\phi_F(\mu))]\}, \tag{3}$$

where uppercase denotes Fourier transform of the function in lowercase.

In a kth-law processor, parameter k defines the strength of the applied nonlinearity and determines the performance features of the processor [14]. We carried out computer simulations to establish the value of parameter k best suited to our verification application. Evaluation of correlation output is carried out by considering the peak-to-correlation (PCE) and the discrimination ratio (DR) metrics [16]. The PCE parameter, defined as the ratio between the maximum intensity peak value and the total energy of the output plane, usually indicates the sharpness and height of the output correlation peak. The DR corresponds to the ratio between the maximum peak value of the correlation output, cc, and the maximum autocorrelation peak value of the reference target, ac. It informs about the system's capacity for discerning small differences.

Figure 3 plots the PCE curves versus the expected number of photons, N_p, for different k values when functions $f_{\mathrm{ph}}(x)$ and $f(x)$ are compared by correlation. The PCE value rapidly decreases with the number of photons, particularly when N_p is smaller than 10^7. Intermediate values of k, $k\in[0.2,0.4]$ give the best results in terms of PCE for a small number of photons (below 10^5). We select $k=0.3$, which offers sharp and intense correlation peaks with a fairly good DR. The output correlation plane depicted in Fig. 2(b) is obtained when comparing functions $f_{\mathrm{ph}}(x)$ and $f(x)$. A sharp peak points out over a noisy background. The maximum correlation value is set to unity to make the comparison easier.

To test the discrimination capability of the proposed system, a different text image, $g(x)$ [Fig. 4(a)], is encrypted by using Eq. (1), a photon-limited encrypted function is computed with $N_p=10^3$ [Eq. (2)], and, from this distribution, a decrypted image, $g_{\mathrm{ph}}(x)$, is obtained by using the appropriate key [Fig. 4(b)]. The decrypted image, $g_{\mathrm{ph}}(x)$, is very similar to $f_{\mathrm{ph}}(x)$ [Fig. 2(b)], with a noisy appearance that makes it barely possible to distinguish the original text. Image $g_{\mathrm{ph}}(x)$ is also compared to the original primary image, $f(x)$, through nonlinear correlation [Eq. (3)] to verify its authenticity. Figure 4(c) shows the corresponding correlation plane. In this case, only a noisy background is obtained without any remarkable correlation peak. The maximum normalized intensity value of the correlation plane is 0.14. These

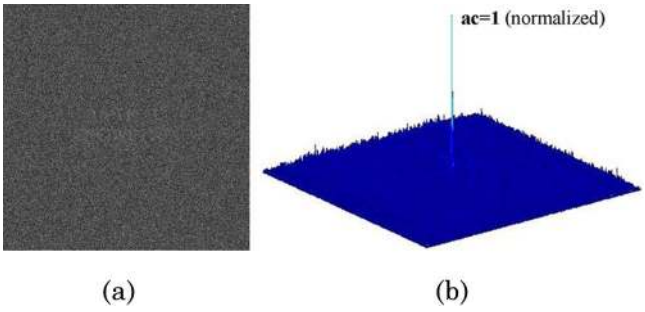

Fig. 2. (Color online) (a) Image $f_{\mathrm{ph}}(x)$. (b) Correlation plane for $k=0.3$.

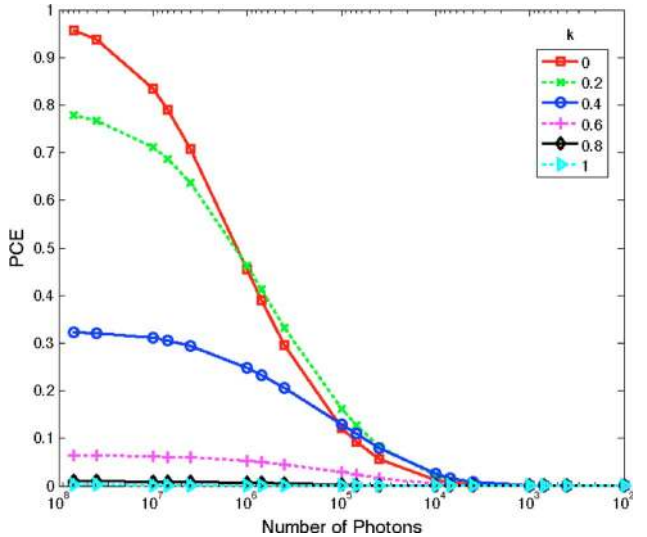

Fig. 3. (Color online) PCE value versus number of photons (N_p) for different nonlinearities (k).

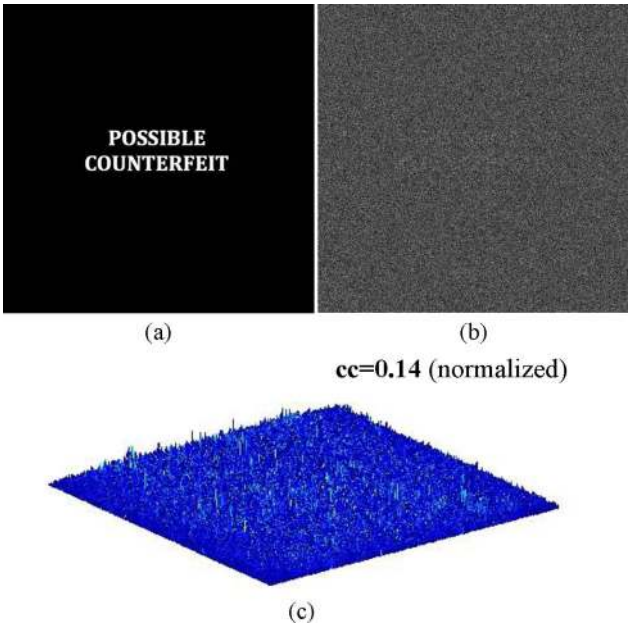

Fig. 4. (Color online) (a) Image $g(x)$; (b) image $g_{\mathrm{ph}}(x)$ for $N_p = 10^3$; (c) correlation plane for $k = 0.3$.

results demonstrate that, on the one hand, it is feasible to authenticate the information decoded from a photon-limited encrypted function [Fig. 2(b)], and, on the other hand, it is possible to discriminate it from other similar images [Fig. 4(c)].

In this Letter we have presented a new image encryption approach by integrating photon-counting imaging and double-random-phase encryption. A sparse encrypted distribution is generated, and the decoded image cannot be recognized by direct visual inspection. Using a reduced number of photons in the encryption process, verification of the encrypted information by nonlinear correlation is demonstrated. This procedure may make it possible to overcome the vulnerability of the DRPE technique to intruder attacks in the sense that the decoded information has a noisylike appearance that makes its visual recognition more difficult.

E. Pérez-Cabré acknowledges the Ministerio de Ciencia e Innovación and Fondo Europeo de Desarrollo Regional (FEDER), project DPI2009-08879, for funding. B. Javidi acknowledges support from the Defense Advanced Research Projects Agency (DARPA).

References

1. B. Javidi and J. L. Horner, Opt. Eng. **33**, 1752 (1994).
2. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
3. D. Weber and J. Trolinger, Opt. Eng. **38**, 62 (1999).
4. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, Appl. Opt. **40**, 2310 (2001).
5. T. Nomura, K. Uota, and Y. Morimoto, Opt. Eng. **43**, 2228 (2004).
6. *Optical and Digital Techniques for Information Security*, B. Javidi, ed. (Springer, 2005).
7. O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, Proc. IEEE **97**, 1128 (2009).
8. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, Opt. Lett. **30**, 1644 (2005).
9. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, Opt. Express **15**, 10253 (2007).
10. E. A. Watson and G. M. Morris, Appl. Opt. **31**, 4751 (1992).
11. G. M. Morris, J. Opt. Soc. Am. A **1**, 482 (1984).
12. S. Yeom, B. Javidi, and E. Watson, Opt. Express **13**, 9310 (2005).
13. J. W. Goodman, *Statistical Optics* (Wiley, 2000).
14. B. Javidi, Appl. Opt. **28**, 2358 (1989).
15. F. Dubois, Appl. Opt. **32**, 4365 (1993).
16. F. Sadjadi and B. Javidi, *Physics of Automatic Target Recognition* (Springer, 2007).
17. A. Mahalanobis, IEEE Trans. AES **45**, 1167 (2009).