DOI: 10.1109/STSIVA.2015.7330460

Secure Image Encryption and Authentication using the Photon Counting Technique in the Gyrator Domain

Juan M. Vilardy O.
Grupo de Óptica e Informática
Universidad Popular del Cesar
Valledupar (Cesar)–Colombia
vilardy.juan@unicesar.edu.co

María S. Millán and Elisabet Pérez–Cabré
Grupo de Óptica Aplicada y Procesado de Imagen
Universitat Politècnica de Catalunya
Terrassa (Barcelona)–Spain
millan@oo.upc.edu, elisabet.perez@upc.edu

Abstract

In this work, we present the integration of the photon counting technique (PhCT) with an encryption system in the Gyrator domain (GD) for secure image authentication. The encryption system uses two random phase masks (RPMs), one RPM is defined at the spatial domain and the other RPM is defined at the GD, in order to encode the image to encrypt (original image) into random noise. The rotation angle of the Gyrator transform adds a new key that increases the security of the encryption system. The decryption system is an inverse system with respect to the encryption system. The PhCT limits the information content of an image in a nonlinear, random and controlled way; the photon-limited image only has a few pixels of information, this type of image is usually known as sparse image. We apply the PhCT over the encrypted image. The resulting image in the decryption system is not a copy of the original image, this decrypted image is a random code that should contain the sufficient information for the authentication of the original image using a nonlinear correlation technique. Finally, we evaluate the peak-to-correlation energy metric for different values of the parameters involved in the encryption and authentication systems, in order to test the verification capability of the authentication system.

1. Introduction

The photon counting technique (PhCT) allows to control the information content of an image in a nonlinear and random form [12, 1]. Recently, the PhCT has been integrated with the double random phase encoding (DRPE) in the Fourier domain [9, 6], for secure image encryption and authentication [7, 5, 8]. The PhCT introduces a nonlinearity into the DRPE system, this nonlinearity increases the security of the encryption and authentication systems against to some attacks [8]. The PhCT can be applied to the original image or encrypted image. On the one hand, if the PhCT is applied to the original image, a photon-limited image with only few pixels is obtained. This image permits to hide the secret information of the original image from visual inspection (information hiding) [7]. On the other hand, if the PhCT is applied to the encrypted image, a sparse encrypted distribution is produced, and a reduction of the transmitted/stored information is achieved (information compression) [7].

In this work, the integration of the PhTC with the DRPE in the Gyrator domain (GD) for secure image authentication is presented. We apply the PhCT over the encrypted image with the purpose of compressing this image. The authentication system is based on a nonlinear correlation technique [2, 3]; in this system the decrypted image is compared with the original image to verify its authenticity. We show that the peak-to-correlation energy (PCE) [11] is improved for certain values of the rotation angle of the Gyrator transform (GT) and the nonlinearity applied in the correlation technique, in comparison with the previous results of the PCE for the integration of the PhTC with the DRPE in the Fourier domain (FD). This improvement over the PCE metric allows a better verification capability for the authentication system.

The paper is organized as follows: Section 2 and 3 introduce the GT and PhCT, respectively. The integration of the PhCT with the DRPE in the GD for secure image authentication is described and illustrated with an example in Section 4. In Section 5, we evaluate and compare the PCE metrics for the integration of the PhCT with the DRPE in the FD and GD. Conclusions are outlined in Section 6.

2. Gyrator transform (GT)

The GT is mathematically defined as a linear canonical integral transform which produces the twisted rotation in position–spatial frequency planes of phase space [10]. The GT at parameter α, which is the rotation angle, of a two-dimensional function $f(x, y)$ can be written in the following

form

$$f_\alpha(u,v) = \mathscr{G}^\alpha\{f(x,y)\} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)K_\alpha(u,v,x,y)\mathrm{d}x\mathrm{d}y, \quad (1)$$

$$K_\alpha(u,v,x,y) = \frac{e^{i2\pi[(uv+xy)\cot\alpha-(vx+uy)\csc\alpha]}}{|\sin\alpha|}, \quad (2)$$

$$\alpha = \frac{p\pi}{2}, \quad \text{where: } 0 \le \alpha < 2\pi, \text{ and } 0 \le p < 4, \quad (3)$$

where x and y denote the coordinates at the spatial domain, u and v indicate the output coordinates in the GD and K_α is the gyrator kernel. For $p = 0$ ($\alpha = 0$), it corresponds to the identity transform. For $p = 1$ ($\alpha = \pi/2$), it reduces to the direct Fourier transform with rotation of the coordinate at $\pi/2$. For $p = 2$ ($\alpha = \pi$), the reverse transform is obtained. For $p = 3$ ($\alpha = 3\pi/2$), it corresponds to the inverse Fourier transform with rotation of the coordinate at $\pi/2$. The GT has a period of 4 with respect to p and 2π for α. The inverse GT corresponds to the GT at rotation angle $-\alpha$. The GT is additive with respect to the rotation angle, $\mathscr{G}^\alpha\mathscr{G}^\beta = \mathscr{G}^{\alpha+\beta}$.

3. Photon Counting Technique (PhCT)

We can control the expected number of incident photons (counts, N_p) over a captured image by using the PhCT. Therefore, in general, a photon-limited image has less information than the original counterpart [7]. The probability of counting l_j photons at pixel j can be shown to be Poisson distributed [12, 1]

$$P_d(l_j;\lambda_j) = \frac{[\lambda_j]^{l_j}e^{-\lambda_j}}{(l_j)!}, \quad l_j = 0,1,2,..., \quad (4)$$

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

The PhCT can be applied to a real-valued image $f(x)$ or the complex-valued image $d(x)$ [7]. For the case of the real-valued image $f(x)$, we obtain the photon-limited image $f_{ph}(x)$ when the equation (4) is applied to the normalized distribution $g(x) = f(x)/\sum_{j=1}^{M} f(x_j)$.

When the PhCT is applied to the complex-valued image $d(x)$, a photon-limited amplitude information $|d(x)|$, is generated from the normalized amplitude image $g(x) = |d(x)|/\sum_{j=1}^{M}|d(x_j)|$ using the equation (4). The pixels that receive at least one photon count are considered in the photon-limited encrypted function $d_{ph}(x)$. Only these pixels contain information of the phase of $d(x)$.

4. Integration of the PhCT with the DRPE in the GD for Secure Image Authentication

We describe the encryption system based on a DRPE in the GD. Let $f(x,y)$ be the real image to be encrypted (original image) with values in the interval $[0,1]$, and $r(x,y)$ and $h_\alpha(u,v)$ be two random phase masks (RPMs) given by

$$r(x,y) = \exp\{i2\pi m(x,y)\}, \quad h(u,v) = \exp\{i2\pi n(u,v)\}, \quad (5)$$

where $m(x,y)$ and $n(u,v)$ are normalized positive functions randomly generated, statistically independent, uniformly distributed in the interval $[0,1]$ and defined at the spatial domain and the GD, respectively. In the first step of the encryption system, the original image $f(x,y)$ is multiplied by the RPM $r(x,y)$ and this product is gyrator transformed with the rotation angle α. The result of the previous GT is multiplied by the RPM $h(u,v)$ and finally, this last product is gyrator transformed with the rotation angle $-\alpha$. The final encrypted image $e(x,y)$ is a complex-valued image defined by

$$e(x,y) = \mathscr{G}^{-\alpha}\left\{h(u,v)\mathscr{G}^{\alpha}\{f(x,y)r(x,y)\}\right\}. \quad (6)$$

The complex-valued encrypted image $e(x,y)$ has amplitude $|e(x,y)|$ and phase $\phi_e(x,y)$ information, so this image can be written as $e(x,y) = |e(x,y)|\exp\{i\phi_e(x,y)\}$. The security keys of the encryption system are given by the rotation angle α of the GT and the RPM $h(u,v)$. These keys will be required for decryption.

In order to obtain a photon-limited encrypted image $e_{ph}(x,y)$, we applied the PhCT with a number of photon counts N_p over the complex-valued encrypted image $e(x,y)$ using the procedure described in the section 3.

The decryption system uses the reverse process of the encryption system. The inputs of the decryption system are: the photon-limited encrypted image $e_{ph}(x,y)$, the rotation angle α of the GT and the RPM $h(u,v)$. In the first step of the decryption system, we apply the GT with the rotation angle α to $e_{ph}(x,y)$ and this result is multiplied by the complex conjugate of the RPM $h(u,v)$. The resulting product is gyrator transforming with the rotation angle $-\alpha$ and finally, we obtain the decrypted image $f_{ph}(x,y)$ when the absolute value function is applied to the last result of the GT. The real-valued decrypted image $f_{ph}(x,y)$ is given by

$$f_{ph}(x,y) = \left|\mathscr{G}^{-\alpha}\left\{h^*(u,v)\mathscr{G}^{\alpha}\{e_{ph}(x,y)\}\right\}\right|, \quad (7)$$

where the superscript * denotes the complex conjugation operation.

The digital results of the encryption system, the PhCT and the decryption system following the steps described above are illustrated with an example in figure 1. The original image $f(x,y)$ has 512×512 pixels and it is presented in

figure 1(a). The random distribution code $m(x, y)$ of RPM $r(x, y)$ is shown in figure 1(b). The random code image $n(u, v)$ of RPM $h(u, v)$ has different values but the same appearance of the image presented in figure 1(b). The amplitude and phase information of the encrypted image $e(x, y)$ are depicted in figures 1(c) and 1(d), respectively, for the rotation angle $p = 3/4$ ($\alpha = 3\pi/8$). Figure 1(e) shows the amplitude of the photon-limited encrypted image $|e_{ph}(x, y)|$, corresponding to figure 1(c) when the total number of photon counts for the PhCT is set to be $N_p = 10^3$. The decrypted image $f_{ph}(x, y)$ for all the correct keys ($h(u, v)$ and α) is shown in figure 1(f). The digital GT was implemented using the fast algorithm of the discrete GT based on convolution operation [4].

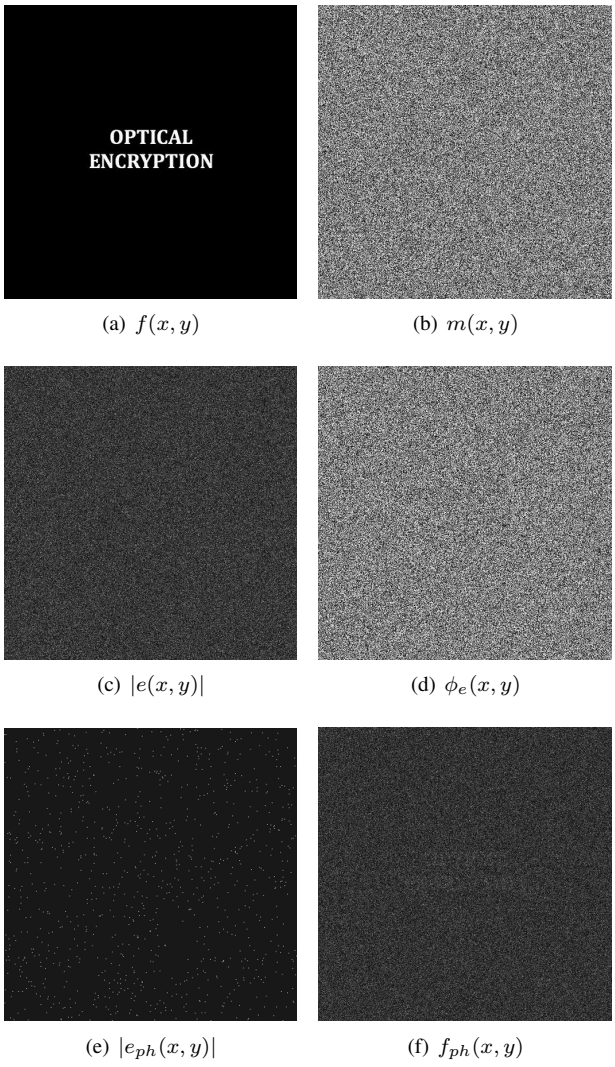
The encrypted image $e(x, y)$ looks like random noise that protects the information content of the original image, as can be seen in figures 1(c) and 1(d). The amplitude of the photon-limited encrypted image $|e_{ph}(x, y)|$ shown in figure 1(e) is a sparse version of the amplitude encrypted image $|e(x, y)|$. The total number of photons in figure 1(e) is $N_p = 10^3$, which corresponds to less than 0.4% of the total number of pixels of the 512×512 original image. The decrypted image $f_{ph}(x, y)$ of figure 1(f) is a random real-valued image that it is not a copy of the original image. The text contained in the original image of figure 1(a) cannot be recognized from the noisy decrypted image $f_{ph}(x, y)$ depicted in figure 1(f). Therefore, the decrypted image $f_{ph}(x, y)$ is not intended for visualization, but it has sufficient information for authentication [7].

The authentication process of the decrypted image $f_{ph}(x, y)$ compares this image with the original image $f(x, y)$ utilized as a reference, by using a nonlinear correlation technique [2]. The images to be compared are Fourier transformed, nonlinearly modified and multiplied in the FD. By inverse Fourier transforming this product, the nonlinear correlation $c(x, y)$ between both images is obtained [2]

$$c(x, y) = \mathscr{F}^{-1}\left\{ \frac{\mathscr{F}\{f(x, y)\}\left[\mathscr{F}\{f_{ph}(x, y)\}\right]^*}{\left|\mathscr{F}\{f(x, y)\}\right|^{1-k}\left|\mathscr{F}\{f_{ph}(x, y)\}\right|^{1-k}} \right\}, \tag{8}$$

where the parameter k defines the strength of the applied nonlinearity and determines the performance features of the correlator [2]. The parameter k is defined in the interval $[0, 1]$.

The intensity output for the nonlinear correlation $c(x, y)$ with $k = 0$, between the decrypted image $f_{ph}(x, y)$ of figure 1(f) and the reference original image $f(x, y)$ of figure 1(a) is presented in figure 2. This result allows the authentication of the decrypted image $f_{ph}(x, y)$ due to the sharp peak presented in the output correlation $c(x, y)$ over its noisy background. The maximum correlation value has been set to unity to make the comparison easier.



(a) $f(x, y)$ (b) $m(x, y)$

(c) $|e(x, y)|$ (d) $\phi_e(x, y)$

(e) $|e_{ph}(x, y)|$ (f) $f_{ph}(x, y)$

Figure 1. (a) Original image $f(x, y)$ to be encrypted. (b) Random image $m(x, y)$ of RPM $r(x, y)$. Encrypted image $e(x, y)$ for the rotation angle $p = 3/4$ ($\alpha = 3\pi/8$): (c) Amplitude information $|e(x, y)|$, and (d) Phase information $\phi_e(x, y)$. (e) Amplitude information of the photon-limited encrypted image $|e_{ph}(x, y)|$ with $N_p = 10^3$, and (f) Real-valued decrypted image $f_{ph}(x, y)$.

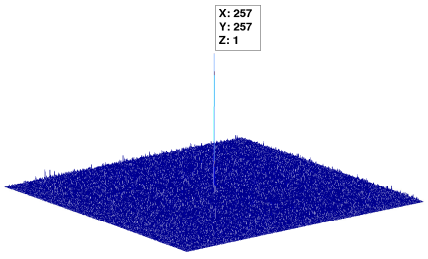
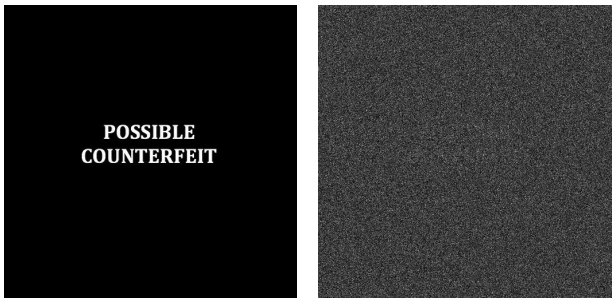
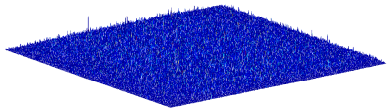


Figure 2. Intensity output for the nonlinear correlation $c(x, y)$ between the decrypted image $f_{ph}(x, y)$ of figure 1(f) and the original image $f(x, y)$ of figure 1(a) with $k = 0$.



(a) $\tilde{f}(x,y)$ (b) $\tilde{f}_{ph}(x,y)$



(c) $\tilde{c}(x,y)$

Figure 3. (a) False image $\tilde{f}(x,y)$ to be encrypted. (b) New decrypted image $\tilde{f}_{ph}(x,y)$ from a photon-limited encrypted image $\tilde{e}_{ph}(x,y)$ with $N_p = 10^3$, and (c) Intensity output for the nonlinear correlation $\tilde{c}(x,y)$ between the decrypted image $\tilde{f}_{ph}(x,y)$ of figure 3(b) and the original image $f(x,y)$ of figure 1(a) with $k = 0$.

In order to test the discrimination capability of the proposed system, we generate a new decrypted image $\tilde{f}_{ph}(x,y)$ from a false image $\tilde{f}(x,y)$. The new encrypted image $\tilde{e}(x,y)$ is obtained from $\tilde{f}(x,y)$ using the equation (6) for the rotation angle $p = 3/4$ ($\alpha = 3\pi/8$). The photon-limited encrypted image $\tilde{e}_{ph}(x,y)$ is computed with $N_p = 10^3$, and from this image the decrypted image $\tilde{f}_{ph}(x,y)$ is obtained by using the equation (7) and the appropriate keys (the RPM $h(u,v)$ and the rotation angle α of the GT). The false image $\tilde{f}(x,y)$ and the decrypted image $\tilde{f}_{ph}(x,y)$ are shown in figures 3(a) and 3(b). The decrypted image $\tilde{f}_{ph}(x,y)$ of figure 3(b) is very similar to the decrypted image $f_{ph}(x,y)$ of figure 1(f) with a noisy appearance that does not permit to make out the original text.

We compare $\tilde{f}_{ph}(x,y)$ with the original image $f(x,y)$ using the equation 8 (nonlinear correlation) with $k = 0$ to verify its authenticity. The obtained intensity output for the nonlinear correlation $\tilde{c}(x,y)$ is depicted in figure 3(c). For this case, only a noisy background is obtained without any remarkable correlation peak. Thus, it is possible to reject the analyzed image and consider it as a false image.

When an incorrect rotation angle α of the GT or an incorrect RPM $h(u,v)$ or both at the same time are used in the decryption system, the obtained decrypted images $f_{ph}(x,y)$ are still noisy patterns very similar to figures 1(f) and 3(b) and the obtained intensity output for the nonlinear correlations $c(x,y)$ between $f_{ph}(x,y)$ and $f(x,y)$ are noisy background without any sharp peak, similarly to the output plane shown in figure 3(c). These results prove that all the keys of the encryption system are required in the decryption stage for the correct authentication of the decrypted image $f_{ph}(x,y)$.

5. Evaluation of the PCE metric

We use the PCE metric in this section with the purpose of evaluating the verification capability of the proposed system. The PCE metric, defined as the ratio between the maximum intensity peak value of the correlation and the total energy of the output correlation plane, usually indicates the sharpness and height of the output correlation peak [11]. The PCE metric can be defined as

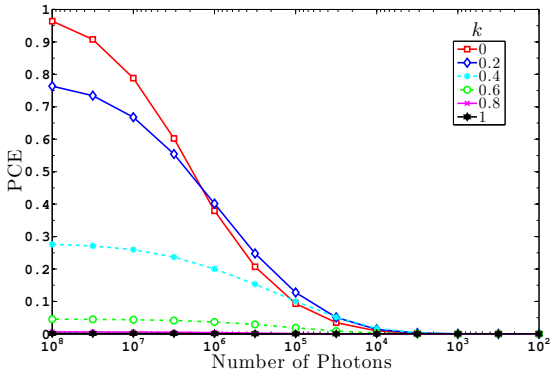
$$\text{PCE} = \frac{\text{AC}_{ph}}{\int |c(x,y)|^2 \, \mathrm{d}x\mathrm{d}y}, \tag{9}$$

where the parameter AC_{ph} represents the maximum intensity peak value of the nonlinear correlation between the decrypted image $f_{ph}(x,y)$ and the original image $f(x,y)$. The PCE metric is evaluated for different values of the number of photons N_p, the nonlinearities k and the rotation angle α of the GT.

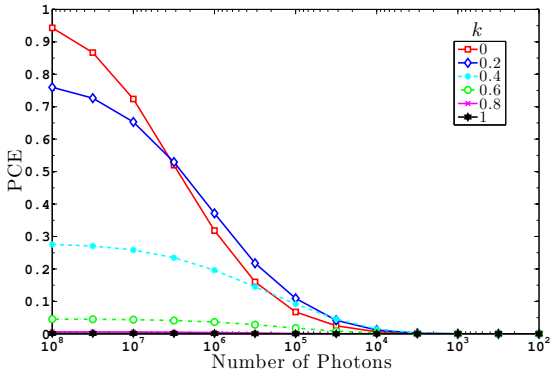
We show the results for the PCE metric in figure 4(a) when the PhCT is integrated with the DRPE system in the FD [7]. The equations (6) and (7) of the DRPE system for encryption and decryption in the GD can be converted into a DRPE in the FD when the GTs of rotation angles α and $-\alpha$ are replaced by the direct and inverse Fourier transform, respectively. In figure 4(a), the PCE values rapidly decrease with the number of photons, particularly when N_p is less than $10^{6.5}$. The values of k between 0.2 and 0.4 give the best results in terms of PCE when N_p is less than 10^5.

Figures 4(b) and 4(c) present the PCE results for the proposed integration of the PhCT with the DRPE in the GD for the rotation angles $p = 0.5$ ($\alpha = \pi/4$) and $p = 1$ ($\alpha = \pi/2$), respectively. The rotation angles $p = 0$ ($\alpha = 0$) and $p = 2$ ($\alpha = \pi$) were unused in the DRPE system in the GD because the results of the GT with these rotation angles for the original image are the same or an inverted original images, respectively, and the encrypted images are not random images. When the PCE is evaluated for a rotation angle p different from 0, 0.5, 1, 2 and 3, the PCE curves obtained are very similar to the curves presented in figure 4(b). The PCE curves obtained for the rotation angle $p = 3$ ($\alpha = 3\pi/2$) are very similar to the curves presented in figure 4(c).

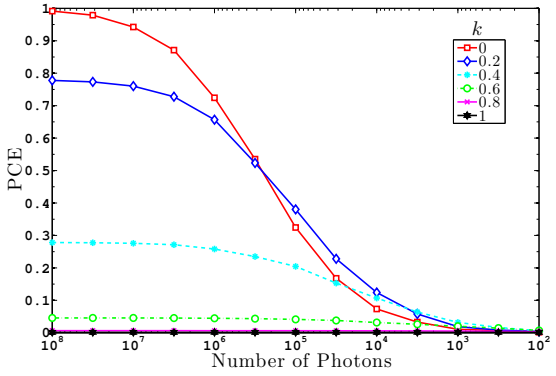
If we compare the results of figures 4(a) and 4(b), we can see that the results of the PCE metric are very similar. On the other hand, the results of the PCE metric from figure 4(c)



(a)



(b)



(c)

Figure 4. PCE values versus number of photons N_p and different nonlinearities k for the integration of the PhCT with the DRPE system in: (a) the FD, (b) the GD for the rotation angle $p = 0.5$ ($\alpha = \pi/4$), and (c) the GD for the rotation angle $p = 1$ ($\alpha = \pi/2$).

with the rotation angles $p = 1$ or $p = 3$ are improved in comparison with the results of the PCE presented in figure 4(a), for the nonlinearities k between 0 and 0.4 and the number of photons $N_p \geqslant 10^{4.5}$. The improvement on the PCE values corresponds to a better verification capability of the authentication system. We recall that the rotation angles $p = 1$ and $p = 3$ of the GT correspond to the direct and inverse Fourier transforms with rotation of the coordinate at $\pi/2$. Therefore, the PCE values can be improved when the rotation angles of the GT are equal to $p = 1$ or $p = 3$ for the integration of the PhCT with the DRPE system in comparison with the PCE values obtained in the integration of the PhCT with the DRPE in the FD.

6. Conclusions

In this paper we have presented the integration of the PhCT with the DRPE in the GD for secure image authentication. We obtained a sparse encrypted image using the GT, DRPE and the PhCT applied to the encrypted image. The decrypted image was a noisy-like code that it is not intended for visualization; this image was utilized for a successful verification of an original image used as a reference pattern by means of a nonlinear correlation technique. The rotation angle of the GT has improved both the security of the encryption system and the PCE metric of the authentication system. The security of the encryption system was improved because a new key, corresponding to the rotation angle of the GT, has been introduced in the DRPE system in comparison with the same encryption system in the FD. The PCE metric of the authentication system was also improved using the rotation angles $p = 1$ ($\alpha = \pi/2$) and $p = 3$ ($\alpha = 3\pi/2$) for the GTs employed in the DRPE system for encryption and decryption.

Acknowledgments

This research has been funded by the Universidad Popular del Cesar from Valledupar (Cesar), Colombia, and the Spanish Ministerio de Ciencia e Innovación and Fondos FEDER (Project DPI2013-43220-R).

References

[1] J. W. Goodman. *Statistical Optics*. Wiley, New York, 2000.

[2] B. Javidi. Nonlinear joint power spectrum based optical correlation. *Appl. Opt.*, 28(12):2358–2367, 1989.

[3] B. Javidi and J. L. Horner. Optical pattern recognition for validation and security verification. *Opt. Eng.*, 33(6):1752–1756, 1994.

[4] Z. Liu, D. Chen, J. Ma, S. Wei, Y. Zhang, J. Dai, and S. Liu. Fast algorithm of discrete gyrator transform based on convolution operation. *Optik*, 122(10):864–867, 2011.

[5] A. Markman and B. Javidi. Full-phase photon-counting double-random-phase encryption. *J. Opt. Soc. Am. A*, 31(2):394–403, 2014.

[6] M. S. Millán and E. Pérez-Cabré. Optical data encryption. In *Optical and Digital Image Processing: Fundamentals and Applications*, pages 739–767. Wiley-VCH Verlag GmbH & Co., 2011.

[7] E. Pérez-Cabré, H. C. Abril, M. S. Millán, and B. Javidi. Photon-counting double-random-phase encoding for secure image verification and retrieval. *J. Opt.*, 14(9):094001, 2012.

[8] E. Pérez-Cabré, E. A. Mohammed, M. S. Millán, and H. L. Saadon. Photon-counting multifactor optical encryption and authentication. *J. Opt.*, 17(2):025706, 2015.

[9] P. Réfrégier and B. Javidi. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.*, 20(7):767–769, 1995.

[10] J. Rodrigo, T. Alieva, and M. L. Calvo. Gyrator transform: properties and applications. *Opt. Express*, 15(5):2190–2203, 2007.

[11] B. V. K. Vijaya Kumar and L. Hassebrook. Performance measures for correlation filters. *Appl. Opt.*, 29(20):2997–3006, 1990.

[12] S. Yeom, B. Javidi, and E. Watson. Photon counting passive 3D image sensing for automatic target recognition. *Opt. Express*, 13(23):9310–9330, 2005.