ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

High secure binary phase multifactor optical ID tag based on photon-counting

Emad A. Mohammed[1*], Elisabet Perez-Cabre[2], H. L. Saadon[1], Maria S. Millan[2],and Hassan H. Mohammed[1]

1. Laser Applications and Optical Materials, Department of Physics, College of Science, University of Basrah, Iraq

2. Applied Optics and Image Processing Group, Department of Optics and Optometry, Technical University of Catalonia, (Barcelona), Spain

Manuscript Info

Manuscript History:

Received: 10 April 2015
Final Accepted: 25 May 2015
Published Online: June 2015

Key words:

Optical security system, binary phase encryption, information authentication, optical ID tags, photon-counting imaging, nonlinear correlation.

Corresponding Author

Emad A. Mohammed

Abstract

We propose, for the first time, multifactor optical ID tag authentication using binary phase encrypted data and photon-counting. We are able to encrypt and compress the primary information contained in the ID tag by applying a binarizing method to the phase data of multifactor encrypted function and combining with photon-counting imaging technique. From this proposal, a binary phase optical identity (BPOID) tag is implemented for authentication. Numerical experiments and results are presented to demonstrate the performance of this ID tag. Cryptanalysis results of the BPOID tag is proved to be anti-counterfeit when applying chosen-plaintext attack (CPA) and is more robust against chosen-cyphertext attack (CCA) based on photon-counting technique.

INTRODUCTION

Optical information processing systems have been widely studied for a number of security applications. These systems involving many tasks such as encryption, recognition, anti-counterfeiting, authentication. The use of biometric images such as fingerprints, face, hand, iris and retina are considered more in authentication than the traditional images. The advantage for optical processing system includes parallel and high-speed processing and multiple degrees of freedom, such as amplitude, phase, wavelength, and polarization [1-6]. Among widely investigated in this field is the double random phase encoding (DRPE) technique [7] under a classical *4f*-optical correlator [8], which is able to encrypt and decrypt an image. An alternative optical security encryption scheme presented to encrypt an original image into a phase-only mask by Wang et al. [9]. The effect of the noise of the encrypted function for DRPE was investigated by Javidi et al. [10]. The robustness of DRPE method against distortions caused by uniform occlusion was demonstrated [11]. For additional security, Towghi et al. proposed a nonlinear DRPE method by converting the input image into a fully phase encoded image [12]. This technique requires strict optical alignment. To overcome this difficultly, a joint transform correlator (JTC) architecture was proposed for DRPE technique [13].

Maria et al. presented multifactor-authentication technique that reinforces optical security by allowing the simulated AND-verification of more than one primary image [14]. The cryptanalysis of DRPE has revealed certain vulnerability against different attacks due to the linearity of 4*f*-processor [15, 16]. Most recently, Perez-Cabre et al. proposed a new system by integrating the photon counting (PC) images technique into DRPE scheme [17]. This is allows to control the number of photons that arrive at a pixel through a Poisson process. A photon-limited encrypted image is very sparse and saved as cyphertext for decryption.

In this paper, we propose a novel multifactor identification for optical security and tagging. In this method, we encrypt the data using the binary phase based multifactor optical encryption authentication with photon counting (PC-MOEA) method. The binary phase is generated by using of dithering method. The data can then be stored in an optical identity (ID) tags, and placed on the object to be authenticated. These ID tags have been shown to be useful tool to achieve, in generally, the different tasks of identification by security validation of the credit cards, passport [18] and remote verification of moving objects to increase the reliability of the security systems [19]. Many ID tag designs have been proposed to increase security and read information under circumstances [20, 21]. However, many of these systems are inherently complex that they use both amplitude and phase regimes of the encrypted information which might limit the practical application. To solve this problem, we avoid amplitude information in the encryption process and work entirely in the phase [22, 23]. In addition, if the optical ID tags are distorted by scratches or cropping, the reconstructed information of symbol images can be distorted, making identification difficult when using a correlation system. Recently, in order to further enhance the security information, Kim presented a simple distortion-invariant optical ID tagging system [24].

The combination of PC-MOEA method applied to the presented binary phase optical identity (BPOID) tag can be useful to a satisfactory authentication and add additional layer of complexity that enhances the security for the verification system of the ID tag against attackers. Numerical experiments and results are presented to demonstrate the performance of the authentication process and cryptanalysis against intruder attacks.

The rest of this paper is organized as follows. In Section 2, a description of the principles for MOEA method and photon counting imaging technique are presented. In Section 3, a novel optical multifactor ID tags are proposed. The performance of the verification for BPOID tag based on PC-MOEA is evaluated in Section 4. The cryptanalysis of the proposed optical ID tags against chosen plaintext and ciphertext attacks is discussed in Section 5. Finally, the main conclusions are presented in Section 6.

2. Encryption and authentication processes

2.1 Multifactor optical encryption authentication

The multifactor optical encryption authentication (MOEA) technique was introduced by Millan et al. [14]. This technique was dedicated to obtain four-factor authentication. The authenticators involve two different primary images and two random phase masks with a combined nonlinear joint transform correlator (JTC) and a classical 4f-correlator [8].

2.1.1 Complex-amplitude encryption function

The complex-amplitude encrypted function of multiple signatures (multifactor) in a single complex-valued distribution $\psi(x)$ is described here. Let $r(x)$ and $s(x)$ denote the reference primary images, and let $b(x)$ and $n(x)$ are the random phase masks used to mask and encrypt the information in the optical ID tag. All the four factors, $r(x)$, $s(x)$, $b(x)$, and $n(x)$, are normalized positive functions distributed over the interval [0,1]. These images can be phase-encrypted yielding $t_r(x)$, $t_s(x)$, $t_{2b}(x)$, $t_{2n}(x)$ that are defined as $t_f(x) = \exp[i\pi f(x)]$. The complex-amplitude encrypted function $\psi(x)$ including the multifactor authenticators will be depicted by the expression [14]:

$$\psi(x) = t_{r+2b}(x) * t_s(x) * F^{-1}[t_{2n}(x)]\,, \qquad (1)$$

where $t_{r+2b}(x) = t_r(x)\,.\,t_{2b}(x) = \exp[i\pi r(x)]\,.\,exp[i2\pi b(x)]$, F^{-1} denotes the inverse Fourier transform, and $*$ denotes the convolution operation.

2.1.2 Optical processor for multifactor verification

The multifactor authentication system involves an optical processor that consists of a combined nonlinear JTC and a classical 4f-correlator for simultaneous verification and authentications of multiple images. The two key phase codes are known by this processor. This optical processor system can be shown in Figure 1.

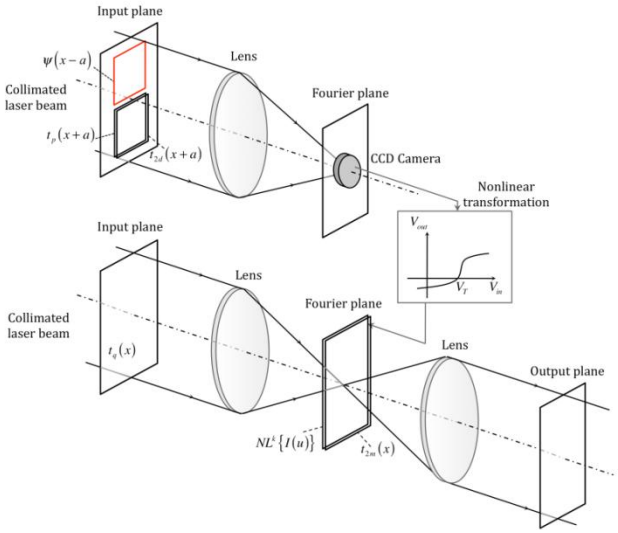


Figure 1. Optical processor for multifactor authentication.

Let *p(x)* and *q(x)* be the positive and normalized input images that are to be compared with those of reference images *r*(*x*) and *s*(*x*), respectively.

In such a case, we have selected the k[th] order nonlinear processor [25] for its simplicity and effectiveness in the experiments, and can be set *k=0* (phase extraction). The resultant nonlinearly modified joint power spectrum is displayed on the Fourier plane of a 4*f*-classical correlator [see Figure 1], where, at the same time, the phase-encoded input image $t_q(x)$ is introduced in the correlator input plane and $t_{2m}(x)$ in the Fourier plane. The interesting term obtained just behind the Fourier plane is [14]

$$\left[T_q(u)T_s^*(u)|T_s(u)|^{k-1}\right]\left[T_{r+2b}^*(u)T_{p+2d}(u)|T_{r+2b}(u)T_{p+2d}(u)|^{k-1}\right][t_{2n}^*(u)t_{2m}(u)]\exp\{i2\pi(2a)u\}, \qquad (2)$$

where a function in uppercase letter indicates the Fourier transform of the function in lowercase letter and u is the spatial frequency coordinate. If the AND condition, *r*(*x*) = *p*(*x*), *s*(*x*) = *q*(*x*), *b*(*x*) = *d*(*x*), and *n*(*x*) = *m*(*x*) is fulfilled and *k=0*, then term of Equation (2) focuses on a sharp multifactor autocorrelation (AC) peak, spatially separated from other terms and centred at *x*=2a corresponding to the cross-correlation of the AC signals given by [14]

$$|AC_{POF}[t_s(x)] \otimes AC_{PPC}^*[t_{r+2b}(x)] \otimes AC_{CMF}^*[T_{2n}(x)] * \delta(x+2a)|^2 \qquad (3)$$

where $\otimes$ is the cross correlation, CMF is the classical matched filter, POF the phase-only filter, and PPC represents the pure phase correlation [26]. It is to be expected that the AC peaks are sharp and narrow intensity. Consequently, the information contained in Equation (2) allows reinforced security verification by simultaneously multifactor authentication.

In addition to that, If any of the authenticator signals do not coincide with the corresponding reference primary image, that is [*p*(*x*) ≠ *r*(*x*) or *q*(*x*) ≠ *s*(*x*)], the output contains a cross-correlation (CC) signal, that is, broader and less intensity than the multifactor AC peak of Equation (2).

2.2 Photon counting imaging

The photon-counting (PC) imaging system was proposed by Perez-Cabre et al. [17, 27]. This system is able to control the expected number of incident photons that arrive at each pixel according to Poisson distribution [17, 28]. By limiting the number of photons, a sparse is appeared. The probability for counting the number of photons at pixels j can be given as [29]

$$p_d(l_j;\alpha_j) = \frac{[\alpha_j]^{l_j} e^{-\alpha_j}}{l_j!}, \qquad l_j = 0,1,2,\ldots\ldots \qquad (4)$$

where l_j is the number of photons detected at pixel j and α_j is the Poisson parameter will be defined as $\alpha_j = N_p g(x_j)$ with $g(x_j)$ is the normalized irradiance at pixel j and N_p is the number of photons in the scene.

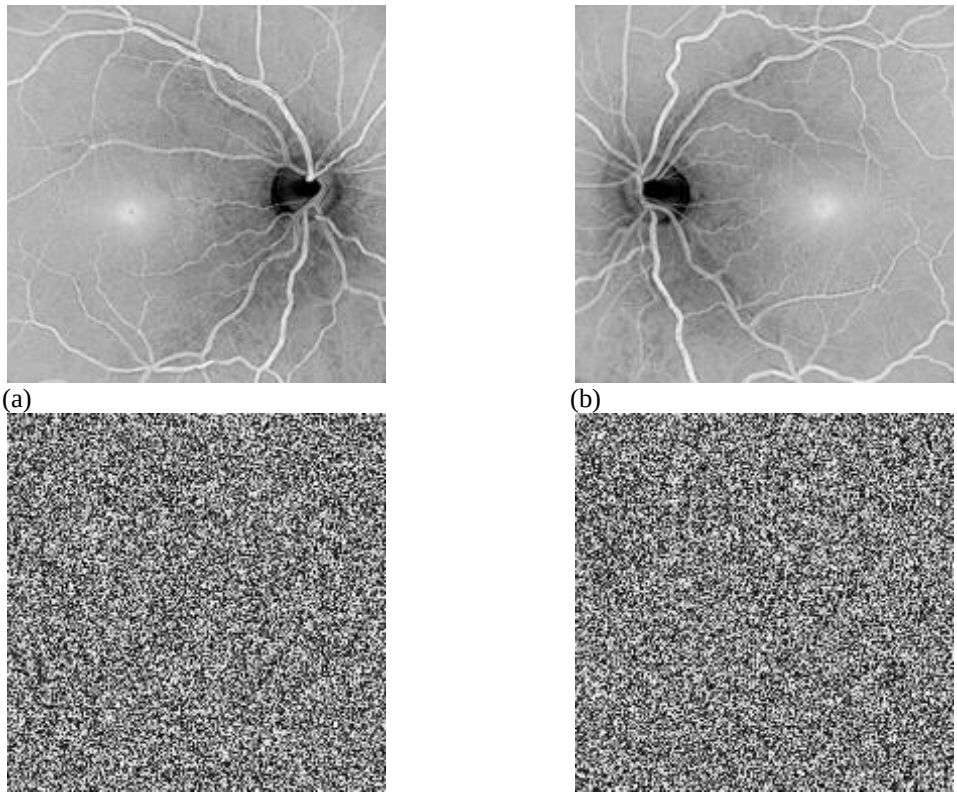
3. Proposed Multifactor Optical ID Tags

In the present work, we combine optical ID tags with the multifactor authentication procedure. Instead of basing the identification on a unique signature or piece of information, our goal is to authenticate a given person by the

simultaneous recognition of several factors. The information of the whole set of factors is included in the ID tag. The optical ID tag includes a reference primary images, an encryption process based on MOEA, and an optical correlation process for verification.

3.1 Encryption Results

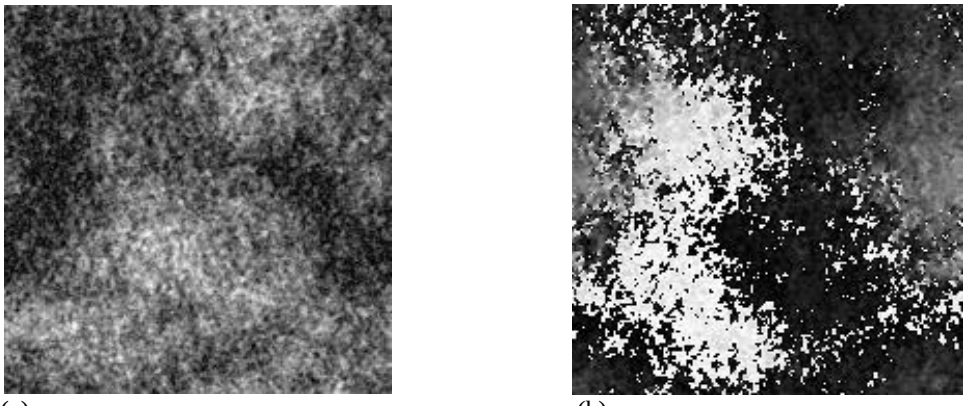
We consider the biometric retina images *r(x) and s(x)* as primary reference images (188 x 188 pixels) and the random phase masks *b(x) and n(x)* as key codes as illustrated Figure 2. From this figure, the encrypted function $\psi(x)$ is obtained by applying Equation (1) [see Figure 3]. Then, the phase only component of an image encrypted with classical MOEA encrypted function will be proposed and the amplitude component remains constant. Therefore, the Figure 3(b) will play the important role in this work.



(a) (b)

(c) (d)

Figure 2. 188 x 188 pixels retina images: (a) right eye *r(x)* and (b) left eye *s(*x), key codes: (c) *b(x)* and (d) *n(x)*.**



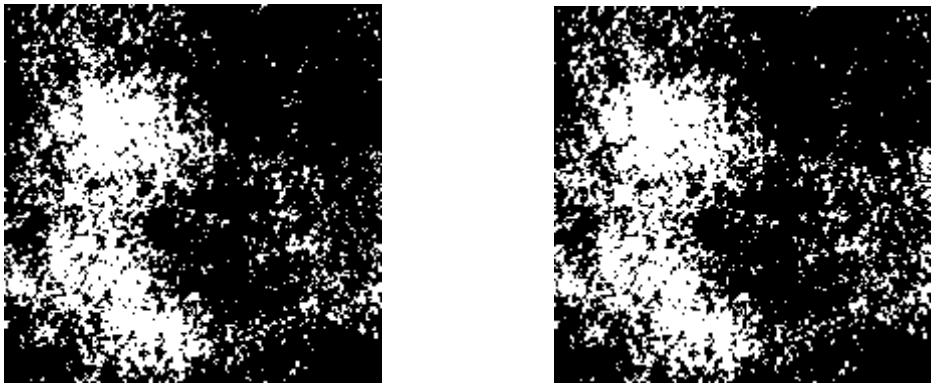
(a) (b)

Figure 3. Encrypted image of the encrypted distribution $\psi(x)$ based MOEA for (a) Magnitude $|\psi(x)|$ and (b) phase $\varphi_{\psi}(x)$.

3.2 ID Tags Synthesis

The optical ID tags presented here are designed for four-factor authentication and must include the information of the encrypted function $\psi(x)$. In the first proposal, the phase only optical encrypted function $\varphi_{\psi}(x)$ is included in the optical ID tag with gray quantization levels as shown in Figure 3(b). The range of gray levels used in the phase encrypted function on the ID tag is 256.

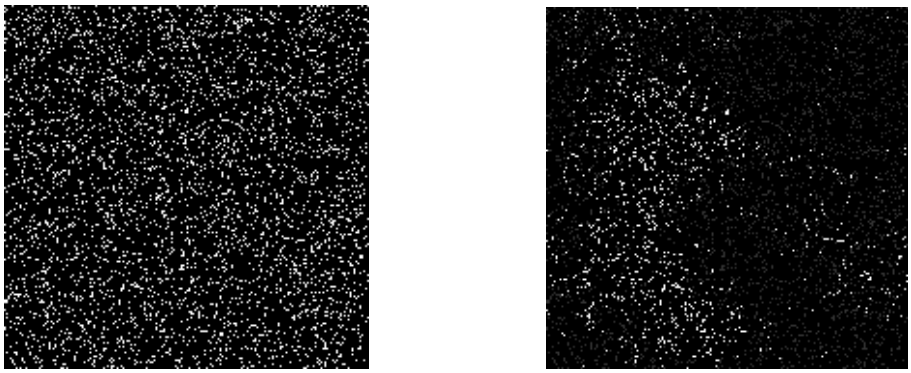
In the second proposal, the range of the gray levels of the phase encrypted function included in the optical ID tag is reduced to two quantized levels (binary levels), so this work actually approaches the manufacturing process for a real ID tag, and would easily overcome the probably difficult situation of ID tag readout in the presence of noise. In a practical application, the reduction in the number of gray levels (or bits) used to reduce the magnitude and phase distribution of the encrypted information on the ID tag will permit to manufacture more versatile and reliable optical ID tag. This reduction is ranged from 8-bit to 1-bit (binary) functions. To compute this effect, the reduction in the number of the bit of ID tag is carried out by considering the compression ratio (C_R), is the ratio between the size of the final function (with respect to the quantization number) and the original size coded on 8-bit, thus; the C_R is 87.5% for binary encoding [30]. A novel ID tag is presented, we call a binary phase optical ID (BPOID) tag. This new ID tag can be achieved by the information of the phase encrypted function $\varphi_{\psi}(x)$. For the BPOID tag based MOEA, a Floyd -Steinberg's error diffusion algorithm method [31] (dithering by Matlab function) is first applied to the phase information, so that it turns out to be a binary distribution. Thus, the dithering phase encrypted distribution, $\varphi_{\psi D}(x)$, is generated from the result in Figure 3(b). The so-obtained data are illustrated in Figure 4(a). For the sake of comparison, another binarization method has been given to the phase information in Figure 3(b). This method is named as a Fixed threshold method [32] and the results are depicted in Figure 4(b). It is known that the results in Figure 4 should be taken (that is, here, $\varphi_{\psi D}(x)$ and $\varphi_{\psi F}(x)$) values of phase. To do that, the results in Figure 4 must be multiplied by π. As seen from Figure 4, the dark and bright pixels represent the phase 0 and 1, respectively.



(a) (b)

Figure 4. Dithering of the gray level phase ID tag for (a) Floyd-Steinberg's error diffusion method and (b) Fixed threshold method.

The last proposal, two integrated procedures of binary phase optical multifactor ID tag and photon-counting imaging technique are used. For the BPOID tag based PC-MOEA, photon counting is applied to the binary phase encrypted image presented in Figure 4 that contains binary phase of the multifactor authenticators. More precisely, we first create a mask image, and then a photon counting is applied to the mask image with number of photons $N_p = 4000$. The mask image is created here, owing to the photon counting is not possible to apply directly to the phase optical ID tag since the phase are distributed in a uniform case. To avoid the interference in the zero values of photon counting and binary phase, the BPOID tag will be shifted by $\pi/4$ to keep the zero values of it. Finally, the photon counting limited mask image to be multiplied by the binary phase encrypted ID tag. The results are shown in Figure 5.

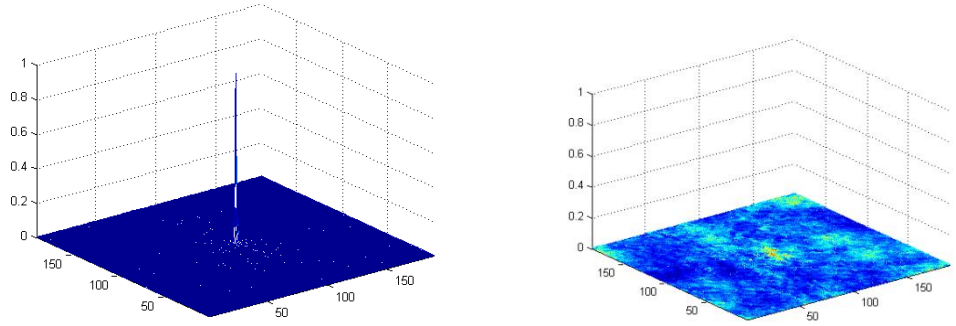


(a) (b)

Figure 5. (a) Photon counting limited mask image with $N_p = 4000$ and (b) photon counting limited for binary phase ID tag.

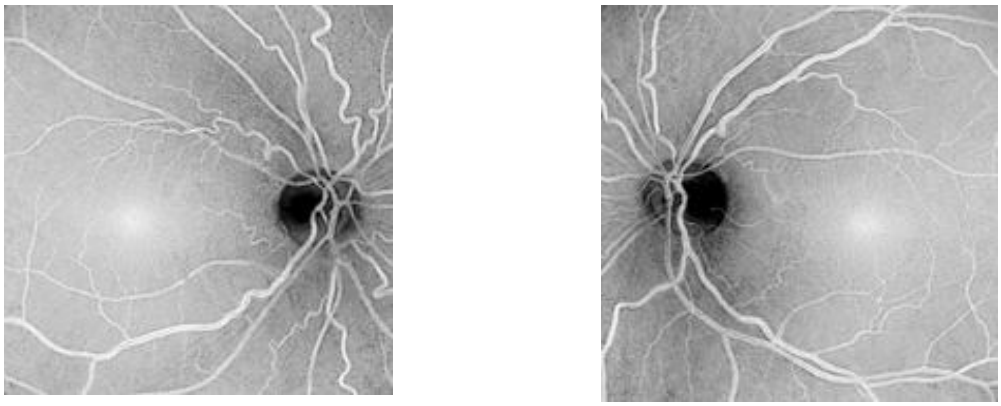
3.3 Authentication Results

To validate the information of gray level phase only optical ID (GPOID) tag, we compute the output correlation intensity distribution of MOEA system with a phase extraction nonlinearity (*k=0)* by using of Equation 2. When all four factor's authentication results are correct, that is, $p(x) = r(x)$, $q(x) = s(x)$, $b(x) = d(x)$ and $n(x) = m(x)$, the normalized output intensity correlation distribution is plotted in Figure 6(a). The obtained results also shows a high and sharp multifactor autocorrelation peak that accounts for a final positive authentication. A negative validation is also shown in Figure 6(b) when another person [see Figure 7], is analyzed by the processor, that is, when $p(x) \neq r(x)$, $q(x) \neq s(x)$ (but still $d(x) = b(x)$ and $m(x) = n(x)$).



(a) (b)

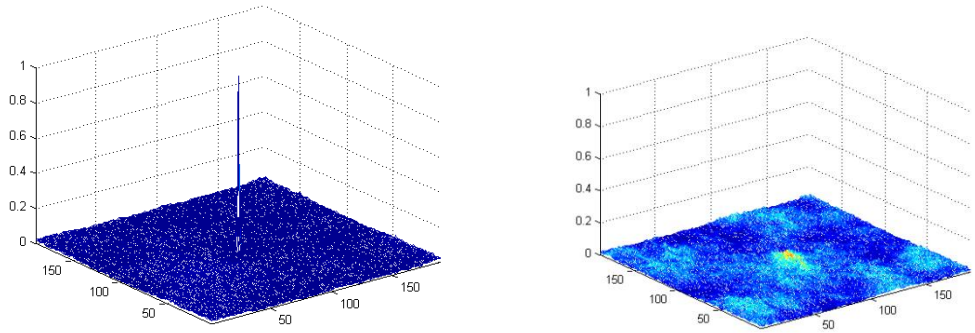
Figure 6. Output correlation intensity distribution for GPOID tag based MOEA with phase extraction (*k= 0*): (a) for positive validation when *p(x) = r(x)* and *q(x)= s(x)* and (b) for negative validation when *p(x) ≠ r(x)* or *q(x) ≠ s(x).* In all cases, RPMs *b(x)* and *n(x)* are correctly provided from the system database.



p(x) *q(x)*

Figure 7. Retina images for the eyes of a non-authorized person.

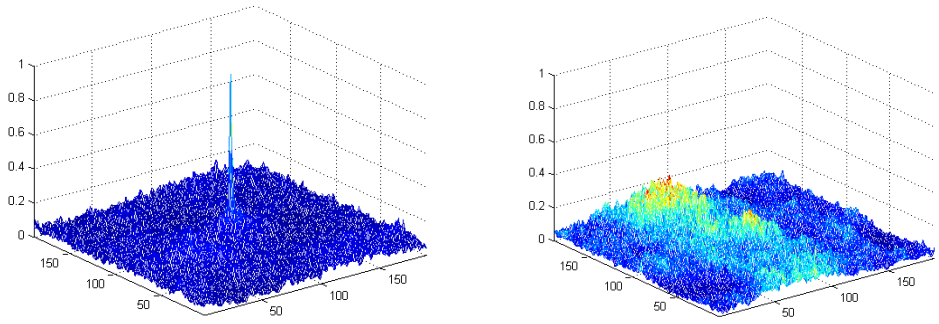
Next, the proposed BPOID tag can be authenticated with phase extraction (*k=0*). When all four factor's authentication results are correct, that is, $p(x) = r(x)$, $q(x) = s(x)$, $b(x) = d(x)$ and $n(x) = m(x)$, then, the normalized output intensity distribution, defined by Equation 2, is shown in Figure 8. Figure 8(a) shows a sharp multifactor auto-correlation peak shape distribution of intensity that allows a compute validation of the set of input images. In the following, if ($p(x) \neq r(x)$ or $q(x) \neq s(x)$) (but still $d(x) = b(x)$ and $m(x) = n(x)$), the output intensity distribution in Figure 8(b) decreases and the peak shape is considerably diminished where the intensity corresponds to the cross-correlation.



(a) (b)

Figure 8. Output correlation intensity distribution for BPOID tag based MOEA with phase extraction (*k= 0*): (a) for positive validation when $p(x)= r(x)$ and $q(x)= s(x)$ and (b) for negative validation when $p(x) \neq r(x)$ or $q(x) \neq s(x)$. In all cases, RPMs $b(x)$ and $n(x)$ are correctly provided from the system database.

Moreover, based PC-MOEA, we have investigated the proposed photon limited BPOID tag. For this purpose, using Equation (4), we have computed the output intensity distribution. Precisely, when the AND condition ($p(x) = r(x)$, $q(x) = s(x)$, $b(x) = d(x)$, $n(x) = m(x)$) is fulfilled, the information contained in the encrypted BPOID tag corresponds to a positive validation, which represents the output intensity that shows a high and sharp multifactor AC peak as plotted in Figure 9(a). While, when the primary image does not match the one included in the photon limited BPOID tag, the output intensity shows a decrease in intensity peak. The so-obtained results are depicted in Figure 9(b).



(a) (b)

Figure 9. Output correlation intensity distribution for BPOID tag based PC-MOEA with phase extraction *k=0* and number of photons $N_p = 4000$: (a) for positive validation when $p(x)=r(x)$ and $q(x)=s(x)$ and (b) for negative validation when $p(x) \neq r(x)$ or $q(x) \neq s(x)$. In all cases, RPMs $b(x)$ and $n(x)$ are correctly provided from the system database.

4. Performance of the Verification for BPOID Tag Based PC-MOEA

To analyze the performance of the proposed BPOID tag based PC-MOEA, the discrimination ratios (DR) and peak-to-correlation energy (PCE) must be given to our verification system [33, 34].

The discrimination ratio (*DR*) metric is defined as the ratio between the maximum peak value of the cross-correlation, *CC*, and the maximum peak value of the autocorrelation, *AC*, [33, 35]

$$DR = \left|1 - \frac{CC}{AC}\right|. \quad (5)$$

It provides information about the capacity of the recognition system for discerning small differences between objects.

The peak-to-correlation energy (*PCE*) parameter, corresponds to the ratio between the maximum intensity peak value and the total energy of the output plane [34, 35]

$$PCE = \frac{correlation\ peak\ energy}{correlation\ plane\ energy}. \quad (6)$$

usually indicates the sharpness and height of the output correlation peak.

In order to select the most appropriate applied nonlinearity (*k*), the discrimination ratio and the peak-to-correlation energy as a function of the number of photons in the scene N_p have been computed at different values of *k*. The results obtained for 20 iteration simulations due to the random process involved in the Poisson distribution, defined by Equation (4), repeated with different parameter values during the photon-counting imaging stage, while the retinal scans, $r(x)$, $s(x)$, $p(x)$ and $q(x)$, as well as the key codes, $n(x)$ and $b(x)$, were kept unchanged. Figure 10 depicts the mean *DR* value computed from the set of numerical simulations versus the number of photon counts N_p with various *k* values. The standard deviations of the numerical simulations permit us to estimate the uncertainties. It is shown clearly from Figure 10 that the DR value rapidly decreases with decreasing the number of photons, particularly when N_p is smaller than of 2000, while, the value of DR increases at number of photons higher than 2000. Moreover, the results show a good discrimination with the number of photons $N_p > 4000$, where the DR > 0.7. For this case, *k=0* and $N_p = 4000$ (or equivalently 11.3% of the image pixels) give the best results in terms of DR and a good recognition for the verification system has been remarked for DR = 0.69.

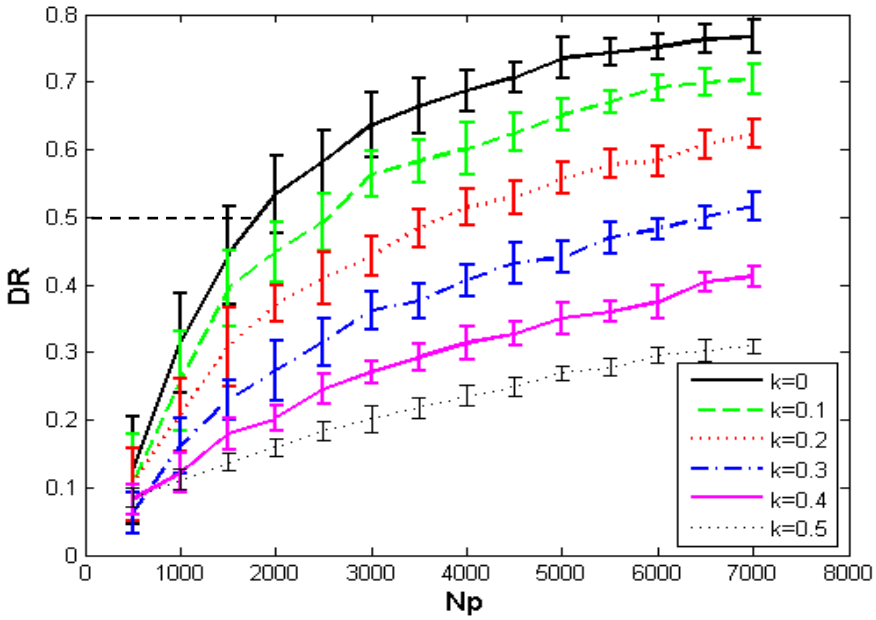


Figure 10. DR versus N_p for BPOID tag based PC-MOEA with different applied nonlinearities (*k* values). The represented values along with their uncertainty bars are established by running 20 numerical experiments of the random process of Poisson distribution in the photon-counting technique and taking the mean value and the standard deviation, respectively.

Figure 11 shows the mean *PCE* values versus N_p for the set of 20 numerical experiments described above. From this figure, it can be observed that the PCE increases semi-linearly for all tested *k* values. *PCE* increases for increasing N_p photon-counts and has a high value at *k=0*.

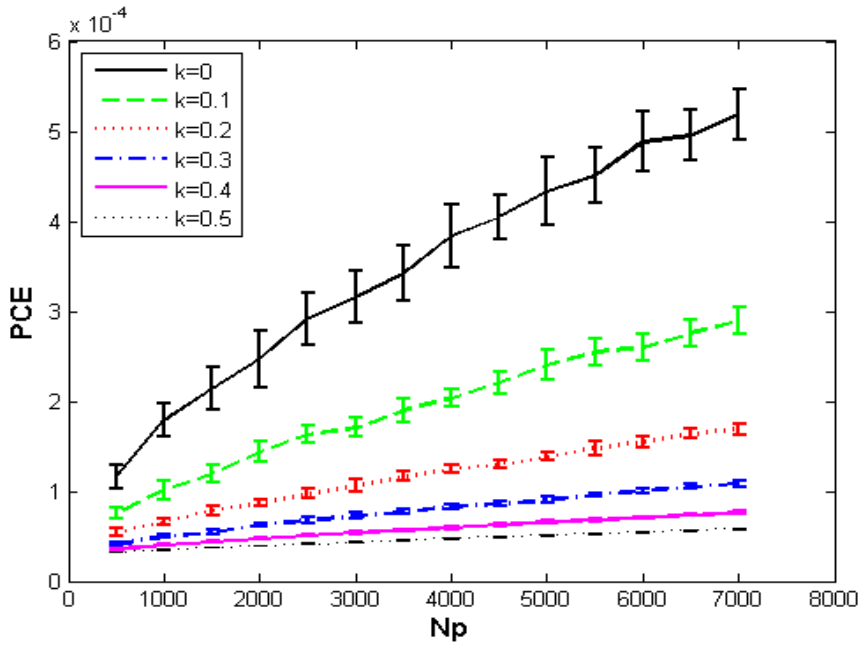


Figure 11. PCE versus N_p for BPOID tag based PC-MOEA with different applied nonlinearities (*k* values). Values and their uncertainties are computed as in Figure 10.

According to the results described in Figures 10 and 11 for the values of DR and PCE, the *k=0* and $N_p = 4000$ offer sharp and intense correlation peaks with a good DR and can be considered for further numerical simulations presented in this work.

5. Cryptanalysis of the Proposed Optical ID Tags

The security of optical ID tags can be revealed against different chosen text attacks. The chosen-plaintext attack (CPA) is defined as the attacker has access to probe the encryption machine and to encrypt specific plaintexts [14]. The other type is the chosen-cyphertext attack (CCA) that the attacker has access to the decryption machine [15]. Therefore, the CPA and CCA are tested here at different proposed ID tags. In this analysis, the test will be done for GPOID and BPOID based MOEA and PC-MOEA tags. In this connection, the obtained results for this cryptanalysis are compared to the positive verification of four factors for the tags mentioned above and the two random phase codes, $b(x)$ and $n(x)$, are supposed to be known by the processor. A Dirac delta function will be considered to the cryptanalysis for all the proposed optical ID tags. All the results correspond to the applied nonlinearity (*k=0*) and the figures are shown in 2D and 3D representations.

5.1 Chosen-Plaintext Attacks

First, let us consider that an unauthorized user has access to the encryption part of the system (that is, trying to counterfeiting the ID tag). In this case, we consider that the unauthorized user takes a Dirac delta function as an input primary image. Figure 12 corresponds to a counterfeit ciphertext with *r(x) = delta(x)* and *s(x) = delta(x)* compared to the in-situ captured retinal images *p(x) = r(x) and q(x) = s(x)* and the phase codes *d(x) = b(x)* and *m(x) = n(x)* from the database. In these cases, the final verification output has negative validation. That is due to the fact that the maximum intensity values of the output planes are always extremely small and are included in the noisy background of the correlation plane.

We first test the gray level phase only optical ID (GPOID) tag based MOEA as shown in Figure 12(a) where the maximum intensity peaks are normalized to the correct four-factor authentication case shown in Figure 6. From this figure, we observed that in the output verification plane the biometric image used as function *q(x)* in the decryption stage is retrieved and displayed in the background with a little noisy; that is the attacker can recognize at least the nature of the information which for verification.

For BPOID based MOEA, the output authentication planes for CPA is illustrated in Figure 12(b). In this case, the maximum intensity peaks are normalized to the correct four-factor authentication case as shown in Figure 8. As seen,

the results of the Figure 12(b) is different from Figure 12(a) because the BPOID tag does not retrieve the biometric image in the background of negative authentication plane.

When the CPA is applied to the BPOID based PC-MOEA with $N_p = 4000$ and the maximum intensity peaks are normalized to the correct four-factor authentication case as shown in Figure 9, the results are depicted in Figure 12(c).

As a results of the above, it can be concluded that the results for BPOID tag based MOEA and PC-MOEA would lead to anti-counterfeit optical ID tag indicating a robust behaviour against the described CPAs in terms of authentication.

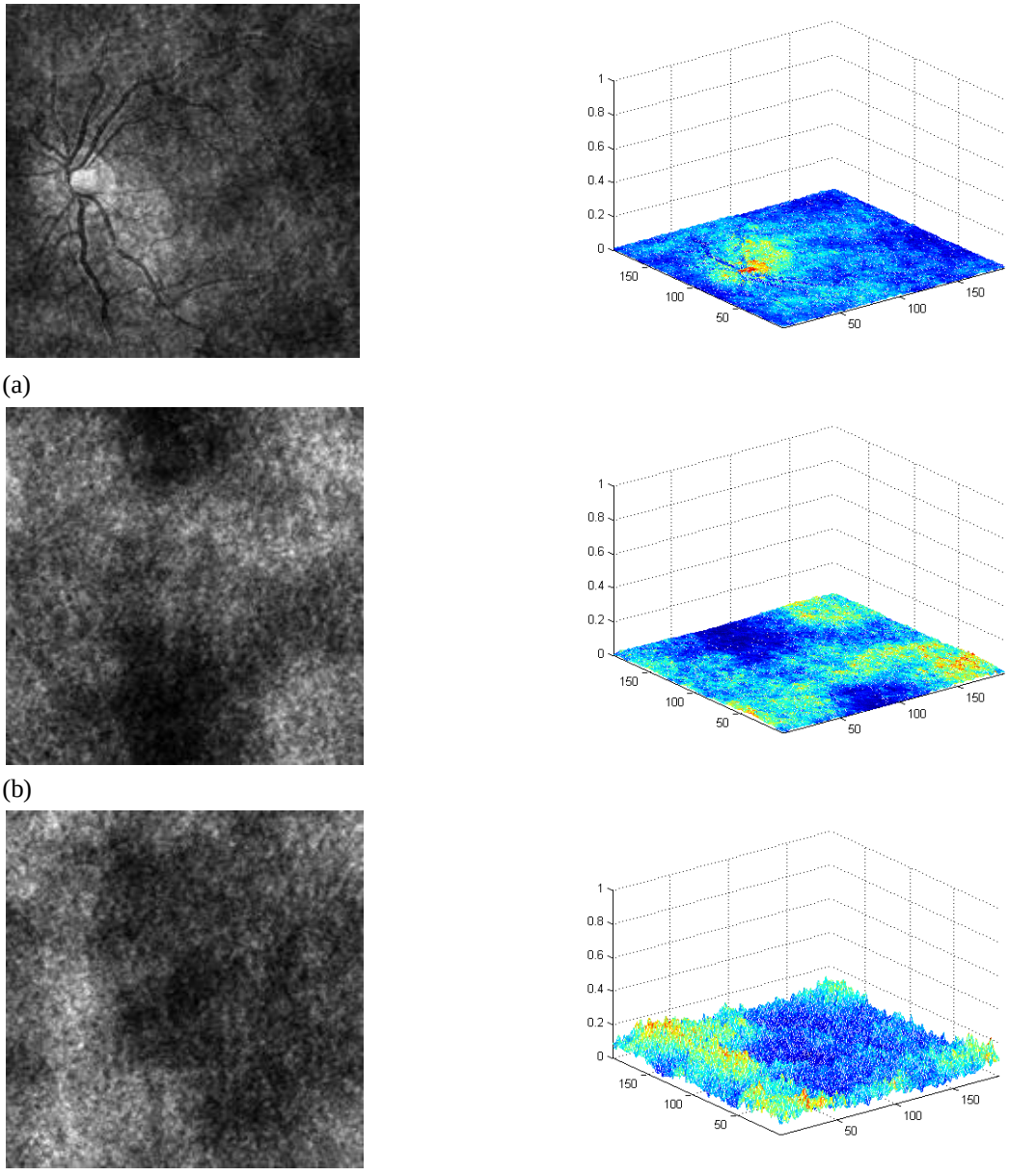


Figure 12. 2D and 3D representation of the output authentication planes when CPA with *r(x) = delta(x)* and *s(x) = delta(x)* for (a) GPOID tag based MOEA, (b) BPOID tag based MOEA, and (c) BPOID tag based PC-MOEA. In all cases, RPMs *b(x)* and *n(x)* are correctly provided from the system database and the nonlinearity *k=0* is applied.

5.2 Chosen-Ciphertext Attacks

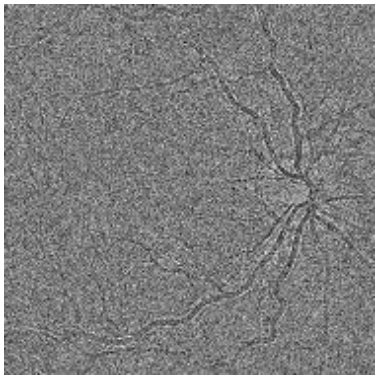
In the second step of cryptanalysis, a user unauthorized access can cause the ID tag to disclosed the decryption machine through the CCA. If the CCA is able to obtain a valid encrypted ID tag with a correct information for four factors, thus, the attacker will try to access the decryption stage by choosing the appropriate signals *p(x)* and *q(x)*. The aim of the attacker is to achieve a positive multifactor validation. In this section, the attacker considers also a Dirac delta function as input images.

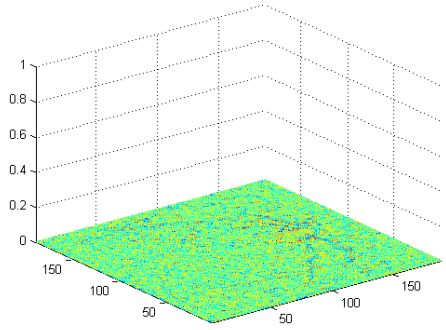
First, for GPOID tag based MOEA, the obtained results for verification system are negative where the maximum intensity peaks are normalized to the correct four-factor authentication case shown in Figure 6. Again the intruder cannot get the positive validation. When (*p(x) = delta(x) and q(x) = delta(x)*), a negative authentication is achieved as a result of the low energy output obtained in this situation but it is displayed a reverse retina *s(x)* in the background of the verification plane as illustrated in Figure 13(a), and hence the attacker can recognize at least the nature of the encrypted information.

In the case of BPOID based MOEA, a similar behavior of reverse retina image *s(x)* is displayed in the background of the output plane for verification stage, but with low lighting in the reverse image in the background of the verification plane. The results are described in Figure 13(b). Here, maximum intensity peaks are normalized to the correct four-factor authentication case shown in Figure 8

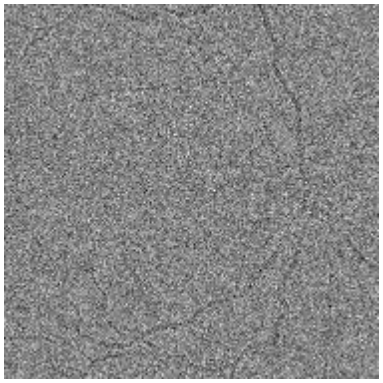
To overcome the problem of partial discloser of confidential information on the background of the output plane, the proposed BPOID based PC-MOEA is applied to solve this problem. The so-obtained results are illustrated in Figure 13(c). Maximum intensity peaks are normalized to the correct four-factor authentication case of BPOID based PC-MOEA with $N_p = 4000$ as shown in Figure 9.

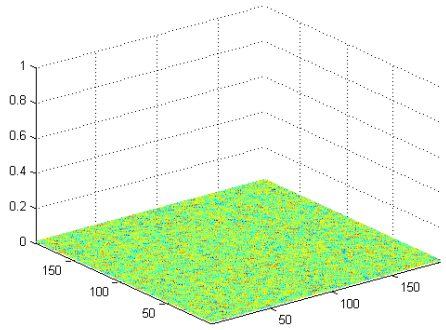
The results have led to the proposed BPOID tag based PC-MOEA to be anti-counterfeit and more secure and robust against chosen-plaintext and chosen-ciphertext attacks, respectively.



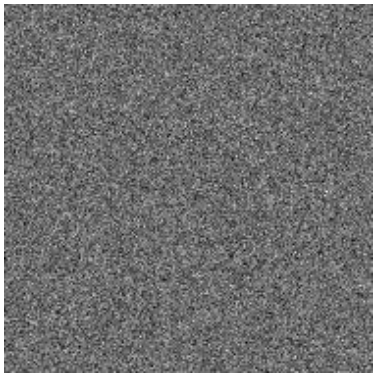


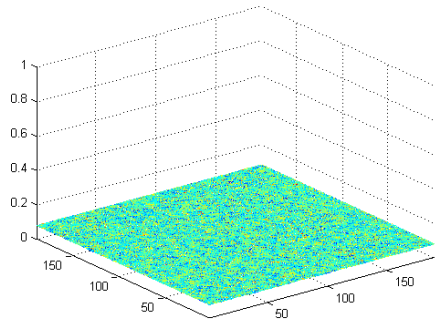
(a)





(b)





(c)

Figure 13. 2D and 3D representation of the output authentication planes when CCA with *p(x) = delta(x)* and *q(x) = delta(x)* for (a) GPOID tag based MOEA, (b) BPOID tag based MOEA, and (c) BPOID tag based PC-MOEA. In all cases, RPMs *b(x)* and *n(x)* are correctly provided from the system database and the nonlinearity *k=0* is applied.

6. Conclusion

We proposed a novel binary phase optical identity (BPOID) by combining binary phase encrypted data with photon-counting imaging technique, for the first time. This procedure adds further compression to the encrypted data and makes difficulty to visually authentication the information contained in the ID tag. This ID tag is easy to implement in practice due to the effect of the binarization of the phase encrypted data, as it consists of only two phase components. In addition, computer simulations of the cryptanalysis results have been shown that the BPOID tag is high robustness against chosen-plaintext attack (which leads to have anti-counterfeit BPOID tag). Moreover, the integration of the PC-MOEA method with BPOID tag led to a verification stage which is more robust against chosen-cyphertext attack and the output plane of the verification system without any displaying of the primary biometric image (retina image). The presented new BPOID tag is more encrypted than the traditional optical ID tags. The integration of the BPOID tag with photon-counting permits to add further compression to the applied ID tag.

Acknowledgements

This work has been partially supported by a Grant from the Iraqi Ministry of Higher Education under the framework of a collaboration between the University of Catalonia, Department of Optics and Optometry (Barcelona, Spain) and the University of Basrah, Department of Physics (Basrah, Iraq).

References

[1] Kumar A, Singh M, and Singh K 2011 Speckle coding for optical and digital data security application: Advances in speckle metrology and related techniques (Ed. G H Kaufmann), (Wiley-VCH).

[2] Javidi B 2005 Optical and Digital Techniques for Information Security (Springer).

[3] Matoba M, Nomura T, Pérez-Cabré E, Millán M S, and Javidi B 2009 Optical techniques for information security Proc. IEEE **97** 1128-1148.

[4] Millán M, and Pérez-Cabré E 2011 Optical data encryption: Optical and Digital Image Processing: Fundamentals and Applications (Eds. G. Cristóbal, P. Schelkens, and H. Thienpont), (Wiley-VCH).

[5] Liu S, Guo C, and Sheridan J T 2014 A review of optical image encryption techniques Opt. & Las. Tech. **57** 327-342.

[6] Chen W, Javidi B, and Chen X 2014 Advances in optical security systems Adv. Opt. Photon. **6** 120-154.

[7] Refregier P and Javidi B 1995 Optical image encryption based on input plane and Fourier plane random encoding Opt. Lett. **20** 767-769.

[8] Goodman J W 2004 Introduction to Fourier Optics (McGraw-Hill), 3rd ed.

[9] Wang R K, Watson I A, and Chatwin C 1996 Random phase encoding for optical security Opt. Eng. **35** 2464-2469.

[10] Javidi B, Sergent A, Zhang G, and Guibert L 1997 Fault tolerance properties of a double phase encoding encryption technique Opt. Eng. **36** 992-998.

[11] Goudail F, Bollaro F, Javidi B, and Refregier P 1998 Influence of perturbation in a double phase-encoding system J. Opt. Soc. Am. A **15** 2629-2638.
[12] Towghi N, Javidi B, and Luo Z 1999 Fully phase encrypted image processor J. Opt. Soc. Am. A **16** 1915-1927.
[13] Nomura T and Javidi B 2000 Optical encryption using a joint transform correlator architecture Opt. Eng. **39** 2031-2035.
[14] Millán M S, Pérez-Cabré E, and Javidi B 2006 Multifactor authentication reinforces optical security Opt. Lett. **31** 721-723.
[15] Frauel Y, Castro A, Naughton T J, Javidi B 2007 Opt. Express **15** 10253.
[16] Carnicer A, Montes-Usategui M, Arcos S, Juvells I 2005 Opt. Lett. **30** 1644.
[17] Pérez-Cabré E, Cho M, and Javidi B 2011 Information authentication using photon-counting double-random phase encrypted images Opt. Lett. **36** 22-24.
[18] Javidi B and Horner J L 1994 Optical pattern recognition for validation and security verification Opt. Eng. **33** 1752-1756.
[19] Javidi B 2003 Real-time remote identification and verification of objects using optical ID tags Opt. Eng. **42** 2346-2348.
[20] Pérez-Cabré E, Millán M S, and Javidi B 2007 Near infrared multifactor identification tags Opt. Express **15** 15615-15627.
[21] Millán M S, Pérez-Cabré E, and Javidi B 2006 High secure authentication by optical multifactor ID tags Proc. SPIE **6394**, 63940J.
[22] Mogensen P and Gluckstad J 2000 Phase-only optical encryption Opt. Lett. **25** 566-568.
[23] Mogensen P and Gluckstad J 2001 Phase-only optical decryption of a fixed mask Appl. Opt. **40** 1226–1235.
[24] Kim C 2010 Simple distortion-invariant optical identification tag based on encrypted binary-phase computer-generated hologram for real time vehicle identification and verification Opt. Eng. **49** 115801-115806.
[25] Javidi B 1989 Nonlinear joint power spectrum based optical correlation Appl. Opt. **28** 2358-2367.
[26] Pérez-Cabré E, Millán M S, and Chalasinska-Macukow K 1998 Dual nonlinear correlation applied to textured and colour object recognition Proc. SPIE **3409** 444-455.
[27] E. Pérez-Cabré E, H. C. Abril H C, and M. S. Millán M S 2012 Photon-counting double-random-phase encoding for secure image verification and retrieval J. Opt. **14** 094001.
[28] Yeom S, Javidi B, and Watson E 2005 Photon counting passive 3D image sensing for automatic target recognition," Opt. Express **13** 9310-9330.
[29] Goodman J W 2000 Statistical optics (John Wiley & Sons, Inc.).
[30] Alfalou A and Mansour A 2009 A new double random phase encryption scheme to multiplex and simultaneous encode multiple images Appl. Opt. **48** 5933-5947.
[31] Floyd R W and Steinberg L 1976 An Adaptive Algorithm for Spatial Gray Scale Proc. SID **17**, 75-77.
[32] Javidi B and Kuo C 1988 Joint transform correlation using a binary spatial light modulator at the Fourier plane Appl. Opt. **27** 663-665.
[33] Millán M S, Pérez-Cabré E, and Chalasinska-Macukow K 1999 Pattern recognition with variable discrimination capability by dual nonlinear optical correlation Opt. Commun. **161** 115-122.
[34] Kumar V and Hassebrook L 1990 Performance measures for correlation filters Appl. Opt. **29** 2997-3006.
[35] Chalasinska-Macukow K, Kotynski R, Pérez-Cabré E, and Millán M S 2005 Dual nonlinear correlation in optical pattern recognition (I): Principle and optoelectronic implementation Opt. Pura Apl. **38** 75-83.