ISSN 1991- 8690 الترقيم الدولي 8690 - 1991

Website: http://jsci.utq.edu.iq Email: utjsci@utq.edu.iq

Influence of external distortions on multifactor optical identification tags with photon-counting

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

[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.

E-mail: emadn73@yahoo.com[*]

Abstract

The multifactor optical ID tag reinforces high security verification purposes for credit cards, passports, and product identification marks. In this applications, the optical ID tag should be robust to external distortions. In this work, we investigate the robustness to external distortions of multifactor optical identification (ID) tag based on multifactor optical encryption authentication (MOEA) method, binarization method, and photon counting (PC) technique. The external distortion caused by a uniform and non uniform occlusion (cropping and scratches) of some pixels of the proposed optical ID tags is investigated. Computer simulations are presented to test the system performance against these types of distortions. The results illustrated that the system is able to validate the ID tags, even under severe distortion and it confirmed that the proposed BPOID tag based on PC-MOEA method is more robust compared with the traditional ID tags to such as cropping and scratches.

Keywords: Optical security system, binary phase encryption, information verification, authentication, optical ID tags, optical recognition, Fourier optics.

تأثير التشوهات الخارجية على البطاقات التعريفية لمتعدد العوامل البصري مع العد الفوتوني

المستخلص

أن علامة الهويه البصريه المتعددة العوامل تعزز أغراض التحقق عالية الأمان مثل بطاقات الائتمان وجوازات السفر والعلامات التعريفية للمنتج. أن هذه العلامه يجب أن تكون ذات مقاومه عاليه ضد التشوهات الخارجية. لقد تم في هذا العمل التحقق من قوة علامة متعدد العوامل المشفره بصريا ضد التشوهات الخارجيه بالأستناد الى نظرية ال MOEA ونظرية ال Binarization وتقنية العد الفوتوني. لقد تم دراسة التشوهات المنتظمه وغير المنتظمه لبعض الوحدات المكونه لصورة البطاقه البصريه بسبب الخدش والقص لبعض أقسام البطاقه. كما تم عرض المحاكاة الحاسوبية لاختبار أداء النظام ضد هذه الأنواع من التشوهات. لقد أثبتت النتائج أن النظام قادر على التحقق من صحة الهويات، حتى في ظل التشوهات الخارجيه كما وتؤكد النتائج التجريبية البصرية أن العلامة المقترحة (BPOID) والمعتمده على PC-MOEA تكون أكثر مقاومة إلى التشوهات الخارجية بسبب الخدوش والقطع مقارنة مع البطاقات التقليدية.

1.Introduction

Information security is an integral part of our lives, due to the most complex operations concerning the property documents, wealth materials, money transfer, data information about the security forces, or secret documents. 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. Other improvement has been developed by fully phase processor [9]. This technique requires strict optical alignment. To overcome this difficultly, a joint transform correlator (JTC) architecture was proposed for DRPE technique [10]. Millan et al. proposed a new technique, named multifactor optical encryption authentication (MOEA) [11]. This technique is designed to obtain four-factor authentication for enhancing the security. Most recently, Perez-Cabre et al. proposed a new system by integrating the photon counting (PC) images technique into DRPE scheme [12]. This technique 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.The optical 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 [13] and remote verification of moving objects to increase the reliability of the security systems [14]. Many ID tag designs have been proposed to increase security and read information under circumstances [15, 16]. 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 [17, 18]. 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. More recently, in order to further enhance the security information, Kim presented a simple distortion-invariant optical ID tagging system [19]. In this paper, we demonstrate the influence of external distortions for multifactor optical ID tags based on MOEA method, binarization method, and photon-counting technique. The encrypted information from such operations can be stored in an optical identity (ID) tags, and placed on the object to be authenticated. Here, four types of optical ID tags are proposed and tested based on some approaches to fulfil the requirements of ideal optical ID tag. The first optical ID tag is based on grayscale complex encrypted data (GCOID). The second optical ID tag is based on grayscale phase only encrypted data (GPOID). The third optical ID tag is based on a binary phase encrypted data (BPOID). The last one is based on the combination of the binary phase data and the photon counting, which 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. Not only does the combination of both techniques increase the resistance of the multifactor security system against intruder attacks, but also a bandwidth reduction is gained for better fulfilling the general requirements of data storage and transmission. Numerical experiments and results are presented to demonstrate the performance of the authentication process and effect of external distortions caused by occlusion of some pixels of these ID tags.

2.Theoretical Background

2.1 Multifactor Optical Encryption Authentication

The multifactor optical encryption authentication (MOEA) was dedicated to obtain four-factor authentication. The authenticators involve two different primary images and two random phase masks with a combined nonlinear JTC and a classical 4f-correlator [8].

2.1.1complex-Amplitude Encryption Function

The complex-amplitude encrypted function of multiple signatures (multifactor) in a single complex-valued distribution ψ(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 [11]:

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

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 Authentication

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 Fig. 1.

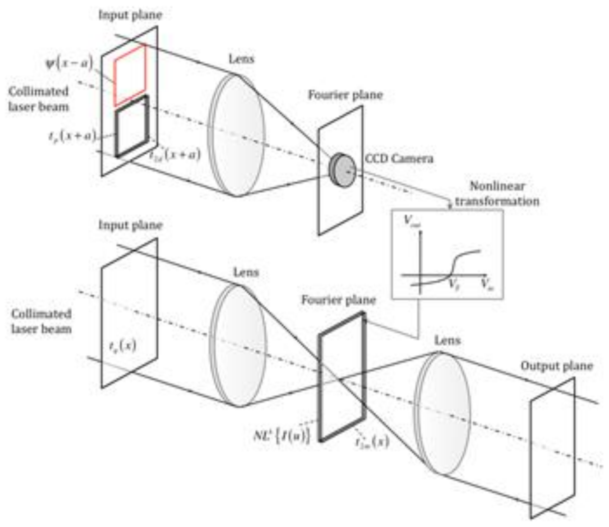


Fig. 1: Architecture of the proposed multifactor optical identity authentication system

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 kth order nonlinear processor [20] 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 4f -classical correlator (Fig. 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 [11]

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

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 Eq. (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 [11]

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

where $\otimes$ is the cross correlation, CMF is the classical matched filter, POF the phase-only filter, and PPC represents the pure phase correlation [21]. It is to be expected that the AC peaks are sharp and narrow intensity. Consequently, the information contained in Eq. (3) 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 Eq. (3).

2.2 Photon-Counting Imaging

The photon-counting (PC) imaging system was proposed by Perez-Cabre et al. [12, 22]. This system is able to control the expected number of incident photons that arrive at each pixel according to Poisson distribution [12, 23]. 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 [24]

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

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. Methods of Preparation

3.1 Encryption Process

We consider the biometric retina images as primary reference images and the random phase masks as key codes. Fig. 2 (a) and (b) show a 188 x 188 pixels biometric retina images used as primary reference images, *r(x)* [right eye] and *s(x)* [left eye], respectively. Fig. 2 (c) and (d) depict the phase masks generated by two random white sequences, *b(x)* and *n(x)*, respectively. Fig. 3 shows the results were obtained the magnitude $|\psi(x)|$ and phase $\varphi_{\psi}(x)$ by applying Eq. (1) to the Fig. 2.

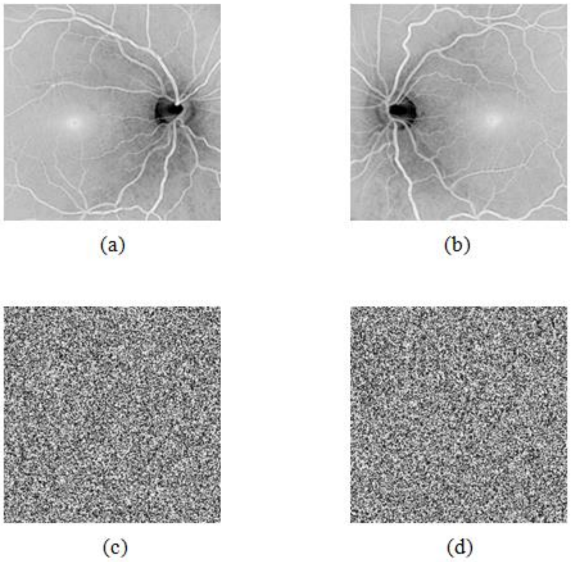


Fig. 2: 188 x 188 pixels retina images: (a) right eye *r(x)* and (b) left eye s(x), key codes: (c) b(x) and (d) n(x)

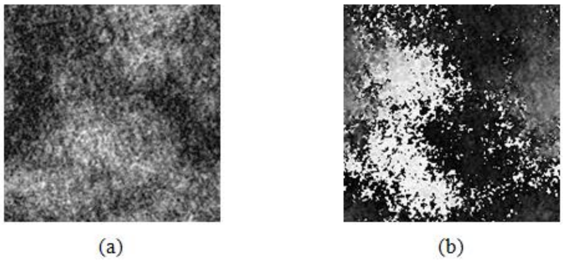


Fig. 3: Encrypted image of the encrypted distribution ψ(x) based MOEA for (a) Amplitude $|\psi(x)|$ and (b) phase $\varphi_{\psi}(x)$

3.2 ID Tags Synthesis

In the first proposal, the optical ID tag is designed to include the information of the encrypted function $\psi(x)$ would be a fully grayscale in this stage and it must be kept both amplitude $|\psi(x)|$ and phase $\varphi_{\psi}(x)$ for verification (GCOID tag).In the second proposal, the phase only optical encrypted function $\varphi_{\psi}(x)$ is included in the optical ID tag with gray quantization levels as shown in Fig. 3(b). The range of gray levels used in the phase encrypted function on the ID tag is 256 (GPOID tag). In the third 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 grey 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 [25]. 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 [26] (dithering by Matlab function) is first applied to the phase information, so that it turns out to be a binary distribution. Thus, the binary phase encrypted distribution, $\varphi_{\psi B}(x)$, is generated from the result in Fig. 3(b). The so-obtained data is illustrated in Fig. 4. It is known that the results in Fig. 4 should be taken (that is, here, $\varphi_{\psi B}(x)$) values of phase. To do that, the results in Fig. 4 must be multiplied by π. As seen from Fig. 4, the dark and bright pixels represent the phase 0 and 1, respectively.

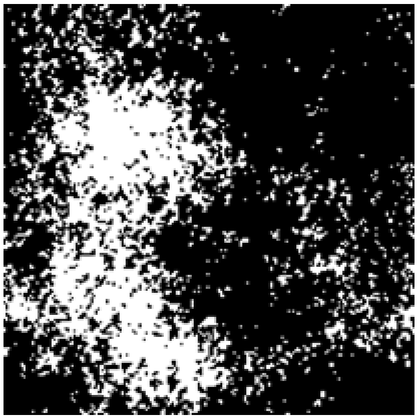


Fig. 4: Binarization of the gray level phase ID tag by Floyd-Steinberg's error diffusion method

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 Fig. 4 that contains binary phase of the multifactor authenticators with number of photons $N_p = 4000$. 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 Fig. 5.

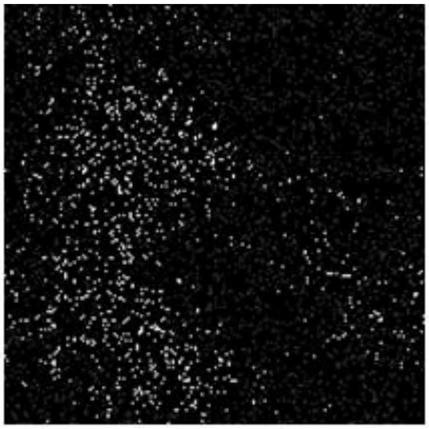


Fig. 5: Photon counting limited image for binary phase optical ID tag with $N_p = 4000$

4. Results and Discussions

4.1 Authentication Results

To validate the information of multifactor optical ID tag, we compute the output correlation intensity distribution of MOEA system with a phase extraction nonlinearity (*k=0)* by using of Eq. 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 Fig. 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 Fig. 6(b) when another person 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 $m(x) = n(x)$).

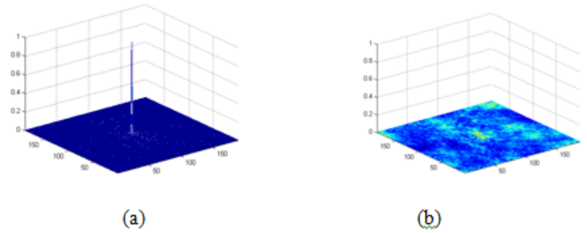


Fig. 6: Output correlation intensity distribution for multifactor optical ID tag with phase extraction (k= 0): (a) for positive validation when p(x)= r(x) and q(x)= s(x) and (b) for negative validation when p(x) ≠ r(x) or q(x) ≠ s(x). In all cases, RPMs *b(x)* and *n(x)* are correctly provided from the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

For comparison, we compute in Table 1 the maximum peak values to output correlation plane for the grayscale complex optical ID (GCOID) tag, the grayscale phase optical ID (GPOID) tag, and the binary phase optical ID (BPOID) tag based MOEA and PC-MOEA, respectively. This table indicates that the output correlation values for GCOID, GPOID, and BPOID tags based MOEA are larger than that when we used PC-MOEA. It is clear that the integration with PC-MOEA will add further compression factor to the encrypted data with fewer photons for authentication. Thus, the output correlation of our proposed BPOID tag is small enough to be able to keep performance of the verification system in spite of highest reduction of the information.

Table 1: Auto-correlation (AC) and Cross-correlation (CC) parameters of GCOID and GPOID tags compared with that the proposed BPOID based on MOEA and PC-MOEA (with *k=0* and $N_p = 4000$), respectively

System	*Maximum peak value*	*Optical ID tag*		
		GCOID	*GPOID*	*BPOID*
MOEA	*AC (a.u.)*	*726*	*253*	*85*
	CC (a.u.)	*7.4*	*4*	*5.7*
PC-MOEA	*AC (a.u.)*	*19*	*6.5*	*13.6*
	CC (a.u.)	*3.2*	*3.7*	*4.2*

4.2 Effects of the External Distortions

In this work, we present two types of distortion that could have an effect in the proposed optical ID tags. Firstly, we discuss the distortions caused by a uniform occlusion (cropping some pixels). Secondly, we check the effect of a non uniform occlusion caused by scratches. Occlusion of the optical ID tag can be implemented as a trial to remove some pixels from the image data. The occlusion of the parts of the ID tag can be modeled as a binary function β, whose value $\beta(x)$ at pixel x is one if this pixel is occluded and zero otherwise. As a result, we can write the occluded ID tag as [27]

$$\psi'(x) = \psi(x) . [1 - \beta(x)]. \qquad (5)$$

The numerical simulations are performed to demonstrate these types of distortions and to illustrate the robustness of the proposed multifactor optical ID tags against such as distortions. To validate the information of the distortion multifactor ID tag, we compute the output intensity distribution with a phase extraction nonlinearity (*k=0*) when all the four-factors are correct, that is, p(x) = r(x) and q(x) = s(x), b(x) = d(x) and n(x) = m(x). The normalized maximum peak value (NMPV) of the output correlation plane is going to be used as an effective measurement metric in the performance of the validation process under these distortions.

4.2.1 Numerical Results for Distortions Cropping

The optical ID tags can be distorted by a uniform occlusion caused by cropping. The occlusion images of the cropping can be shown in Fig. 7. This cropping is generated by using of 25% occlusion at different locations in the entire ID tag symbol.

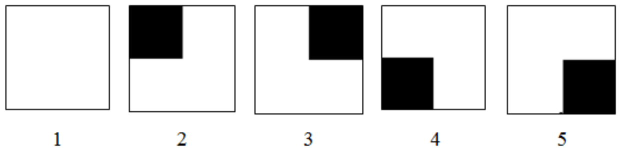
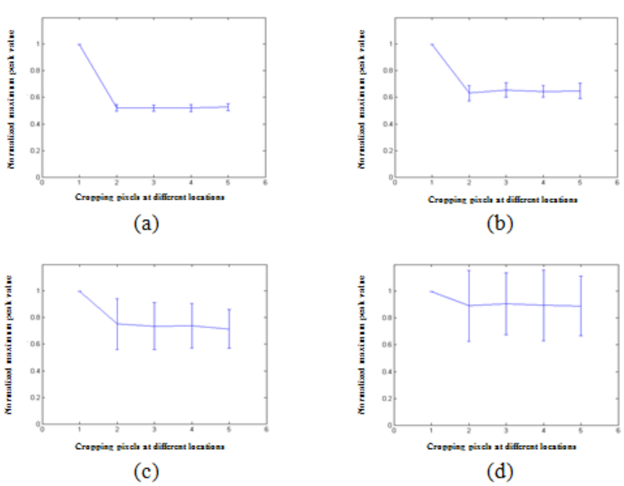


Fig. 7: A uniform occlusion symbols caused by 25% cropping of the total pixels at different locations. The size of the symbols are (188x188 pixels)

After the information lost, the resulting ID tag is used as the input image to the correlator system for verification. Accordingly, to test the effect of the random phase keys (*n*(*x*) and *b*(*x*)) in the proposed optical ID tags, the output distribution intensity for the correlator will be taken for 50 different random phase masks. The obtained results are taken for auto-correlation case when the ID tag includes all the correct four factors, that is, *p(x) = r(x) and q(x) = p(x)* and the RPMs will be fixed for each encryption-authentication process. The reason behind this experiment is to investigate the robustness of the gray scale and binary multifactor optical ID tags. Fig. 8 (a) and (b) show the normalized maximum peak value of the output correlation as a function of the free and 25% cropping at different locations for GCOID and GPOID tags based MOEA. From this figure, we observe a constant degradation of maximum peak value of the output correlation at different location of the cropping of the pixels. A first result of these gray scale ID tags is that the mean for the maximum peak value of the output correlation is linear constant. This behavior indicates that the information lost by 25% is not effective in the performance of the correlation system for the whole ID tags. We also note that no significant standard deviation on these ID tags exists.For the BPOID based MOEA and PC-MOEA, we observe in Fig. 8 (c) and (d) that the mean for the maximum peak value of the output correlation is also linear constant, but it has a high standard deviation due to the reduction of the information by the compression of the binary phase in the BPOID and the additional compression by the photon counting. Furthermore, the MOEA is a unitary process; in other words, it preserves the energy of images. Thus, the effect of photon-counting will be to increase the energy of the decryption image (validation of the optical ID tag).Finally, we can conclude that the location of the occluded pixels caused by cropping has no effect on the performance of the authentication processes for the proposed binary phase ID tags. Consequently, the proposed BPOID based on PC-

MOEA is robust against distortions caused by 25% cropping of the pixels and fulfills the requirement of the compression data.



(a) (b) (c) (d)

Fig. 8: Normalized maximum peak value of the output correlation as a function of the free and 25% cropping at variant locations in the entire ID tag for 50 different of random phase masks: (a) GCOID tag based MOEA, (b) GPOID tag based MOEA, (c) BPOID based MOEA, and (d) BPOID based PC-MOEA at $N_p = 4000$. The nonlinearity k=0 is applied

4.2.2 Numerical Results for Distortions Scratches

When the optical ID tag is distorted by a non uniform occlusion caused by scratches, the symbols images for this scratches can be depicted in Fig. 9. These scratches will occlude the pixels starts from free scratches up to 22.5% scratches of the total pixels in the entire ID tag.

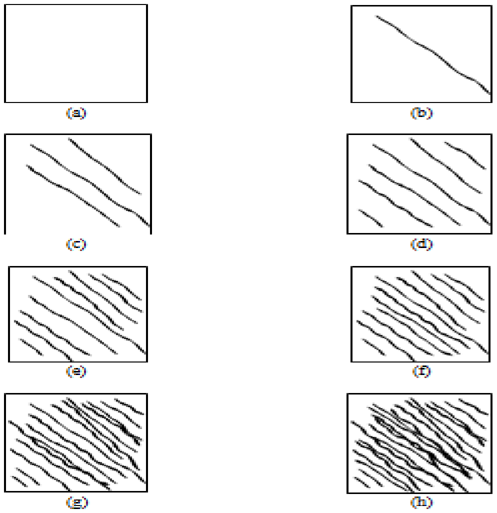
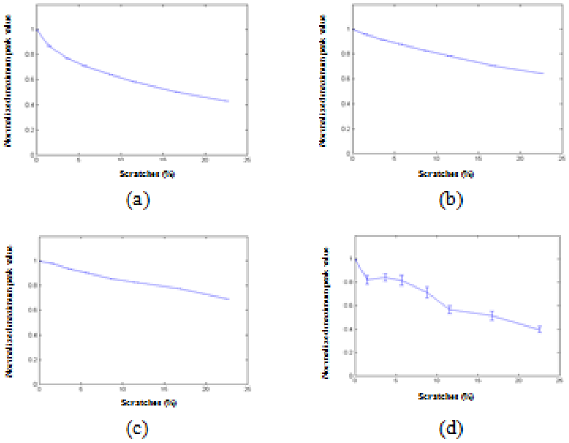


Fig. 9: A non uniform occlusion symbols caused by: (a) Free of scratches, (b) 1.54% scratches, (c) 3.72% scratches, (d) 5.70% scratches, (e) 8.80% scratches, (f) 11.58% scratches, (g) 16.76% scratches, and (h) 22.5% scratches. The size of the symbols are (188x188 pixels)

When the GCOID and GPOID tags are scratched by the occluded images as described in Fig. 9, the verification results of the positive validation in terms of normalized maximum peak value of the output correlation are given in Fig. 10 (a) and (b). From this figure, we have shown that the maximum peak value of output correlation in Fig. 10(a) decreases rapidly (which leads to a low resistance to information loss) and decreases slowly in Fig. 10(b). As we can see from Fig. 10 (a) and (b), even with 22.5% occlusion by scratches the ID tags can be validated and the phase-only multifactor ID tag more robust to information loss in this stage.The validation results for BPOID based MOEA can be illustrated in Fig. 10(c). Fig. 10(c) shows a high resistance to the information loss owing to phase only values and their binarized towards longer noise. For BPOID based PC-MOEA, with $N_p = 4000$, it can be observed that in Fig. 10(d) the ID tag is still being resistance to the information loss. Furthermore, one can note that the validation processes achieve a good performance although the ID tag loss more information due to binary phase process, photon-counting technique and distortions by scratches. Therefore, the result indicates that the proposed binary phase ID tag based PC-MOEA is also robust to such type of scratching.



(a) (b) (c) (d)

Fig. 10: Normalized maximum peak value of the output correlation as a function of the scratches in percentage for: (a) GCOID tag, (b) GPOID tag based MOEA, (c) BPOID tag based MOEA, (d) and BPOID based PC-MOEA tag with $N_p = 4000$. The nonlinearity k=0 is applied

The experimental results, as shown in Figs. 8 and 10, confirmed that the proposed BPOID tag is robust to external distortions such as cropping and scratches. It led to satisfactory results in the verification system. In addition, the BPOID tag based on PC-MOEA can also add further compression factor to the encrypted data with far fewer photons to achieve the requirements of data storage and transmission. Also we demonstrated the effects of distortions (cropping and scratches) using only the phase part of the optical ID tags. Moreover, computer simulations confirmed that the system is able to validate the ID tag, even under severe distortion. For example the system validate the ID tag when 25% of the pixels were occluded.

5. Conclusions

In this paper, we have studied the robustness of the multifactor optical ID tags to the external distortions. The effects of distortions such as occlusion caused by cropping and scratches are demonstrated. The NMPV metric is used to verify the proposed optical ID tags. Computer experiments and results showed that the system is able to validate the proposed optical ID tags although when it is under the external distortions. For example, the system verified the ID tag when 25% of the pixels were occluded. Furthermore, the proposed multifactor BPOID tag based on PC-MOEA method is more secure and robust to the external distortions such as cropping and scratches, even under severe compression of binarization and photon-counting processes.

References

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

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

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

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

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

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

[7] P. Refregier and B. Javidi, 1995 “Optical image encryption based on input plane and Fourier plane random encoding,” Opt. Lett. 20, pp. 767–769.

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

[9] N. Towghi, B. Javidi, and Z. Luo, 1999 “Fully phase encrypted image processor,” J. Opt. Soc. Am. A 16, pp. 1915–1927.

[10] T. Nomura and B. Javidi, 2000 “Optical encryption using a joint transform correlator architecture,” Opt. Eng. 39, pp. 2031-2035.

[11] M. S. Millán, E. Pérez-Cabré, and B. Javidi, 2006 “Multifactor authentication reinforces optical security,” Opt. Lett. 31, pp. 721–723.

[12] E. Pérez-Cabré, M. Cho, and B. Javidi, 2011 “Information authentication using photon-counting double-random phase encrypted images,” Opt. Lett. 36, pp. 22–24.

[13] B. Javidi and J. L. Horner, 1994 “Optical pattern recognition for validation and security verification,” Opt. Eng. 33, pp. 1752–1756.

[14] B. Javidi, 2003 “Real-time remote identification and verification of objects using optical ID tags,” Opt. Eng. 42, pp. 2346-2348.

[15] E. Pérez-Cabré, M. S. Millán, and B. Javidi, 2007 "Near infrared multifactor identification tags," Opt. Express, 15, pp. 15615–15627.

[16] M. S. Millán, E. Pérez-Cabré, and B. Javidi, 2006 "High secure authentication by optical multifactor ID tags," Proc. SPIE 6394, 63940J.

[17] P. Mogensen and J. Gluckstad, 2000 "Phase-only optical encryption," Opt. Lett. 25, pp. 566–568.

[18] P. Mogensen and J. Gluckstad, 2001 "Phase-only optical decryption of a fixed mask," Appl. Opt. 40, pp. 1226–1235.

[19] C. Kim, 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, pp. 115801–115806.

[20] B. Javidi, 1989 "Nonlinear joint power spectrum based optical correlation," Appl. Opt. 28, pp. 2358–2367.

[21] E. Pérez-Cabré, M. S. Millán, and K. Chalasinska-Macukow, 1998 "Dual nonlinear correlation applied to textured and colour object recognition," Proc. SPIE 3409, pp. 444-455.

[22] E. Pérez-Cabré, H. C. Abril, and M. S. Millán, 2012 "Photon-counting double-random-phase encoding for secure image verification and retrieval," J. Opt. 14, 094001.

[23] S. Yeom, B. Javidi, and E. Watson, 2005 "Photon counting passive 3D image sensing for automatic target recognition," Opt. Express 13, pp. 9310-9330.

[24] J. W. Goodman, 2000 Statistical optics, (John Wiley & Sons, Inc.).

[25] A. Alfalou and A. Mansour, 2009 "A new double random phase encryption scheme to multiplex and simultaneous encode multiple images," Appl. Opt. 48, pp. 5933–5947.

[26] R. W. Floyd and L. Steinberg, 1976 "An Adaptive Algorithm for Spatial Gray Scale," Proc. SID 17, pp. 75–77.

[27] F. Goudail, F. Bollaro, B. Javidi, and P. Refregier, 1998 "Influence of perturbation in a double phase-encoding system," J. Opt. Soc. Am. A 15, pp. 2629–2638.