Photon-counting double-random-phase encoding for secure image verification and retrieval

Elisabet Pérez-Cabré[1], Héctor. C. Abril[1], María S. Millán[1], Bahram Javidi[2]

[1] Dept. Òptica i Optometrica, Universitat Politècnica de Catalunya, Violinista Vellsolà 37, 08222 Terrassa (Spain)

[2] Electrical & Computer Engineering Dept., University of Connecticut, 371 Fairfield Road, Unit 2157, Storrs, Connecticut 06269 (USA)

E-mail: elisabet.perez@upc.edu

Abstract. The integration of photon-counting imaging techniques and optical encryption systems can improve information authentication robustness against intruder attacks. Photon-counting imaging generates distributions with far fewer photons than conventional imaging, and provides substantial bandwidth reduction by generating a sparse encrypted data. We show that photon-limited encrypted distributions have sufficient information for successful decryption, authentication and signal retrieval. Additional compression of the encrypted distribution is applied by limiting the number of phase values used to reproduce the phase information of the complex-valued encrypted data. The validity of this technique – with and without phase compression – is probed through simulated experiments for two types of input images: alphanumerical signs and dithered natural scenes.

Keywords: optical security, encryption, photon-counting imaging, nonlinear correlation, information verification, authentication, image retrieval

1. Introduction

Recently, a proposal to integrate the photon-counting imaging technique with optical encryption was presented in Ref. [1]. A photon-limited version of an encrypted distribution, which consists of a sparse representation of the encrypted information, is considered. This sparse representation is used for decryption and, as a result, a noisy decrypted signal, which is not recognizable by visual inspection, is retrieved. By following this procedure, intruders cannot easily recognize the decrypted image retrieved from the sparse encrypted distribution since it is not intended for visualization of the primary image, but for verification of the information by means of optical correlation. Thus, the integration of photon-counting techniques along with double-random-phase encryption (DRPE) [2] introduces an additional layer of information protection that increases the system security and makes the verification process more robust against unauthorized attacks. Other DRPE-based authentication techniques that utilize multiple images, biometric information and near-infrared remote sensing have been developed for a secure multifactor verification [3-4].

In this paper, we further analyse the possibility of combining photon-counting imaging and optical encryption following two alternative schemes for the integration of both techniques. Photon-counting imaging can be applied to the encrypted function as proposed in the previous work [1]. Another approach presented in this work is to apply photon-counting imaging to the primary image prior to its encryption. This paper provides numerical results that show the effect of the reduction of the number of

photons on the verification process and the possibility of reducing the information of the encrypted distribution without affecting the system security. Even though the integration of photon-counting imaging and DRPE was first intended for information verification and not for image visualization, in this paper we present the additional possibility of image retrieval based on the pattern identification obtained from a peaky correlation signal.

Section 2 contains a brief description of both, the photon-counting imaging and the DRPE techniques. Section 3 provides a detailed description of the integration procedure, along with the numerical results that evaluate its technical implementation. Finally, algorithms for information verification and image retrieval are presented in Section 4, prior the conclusions of the work.

2. Background: Photon-Counting Imaging (PhCI); Double-Random-Phase Encryption (DRPE)

2.1 Photon-counting imaging

In photon-counting imaging (PhCI) systems, images can have a limited number of photons by controlling the expected number of incident photons (counts) in the entire scene, N_p [1,5]. Thus, in general, a photon-limited image has less information than the original counterpart. The probability of counting l_j photons at pixel x_j can be shown to be Poisson distributed [6]

$$P_d\left(l_j;\alpha_j\right)=\frac{\left[\alpha_j\right]^{l_j}e^{-\alpha_j}}{l_j!},\quad l_j=0,1,2... \tag{1}$$

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

Figure 1(a) shows a binary image used in the experiments presented in this work. Along with the original primary image, several photon-limited versions are provided in Figure 1(b) to illustrate the effect of limiting the number of photons N_p that reach the image. Photon-limited versions shown in Figure 1(b) hardly reveal the original appearance of the primary image (Fig. 1(a)). For $N_p = 10^4$, which approximately corresponds to 4% of the primary image pixel size, it is possible to slightly make out a text structure on the photon-limited image.

Photon-counting imaging techniques have been applied in many fields and in different spectral bandwidths [5,7-11]. 2D image recognition using photon-limited distributions has also been demonstrated [7-8]. The photon-counting approach on 3D object recognition has recently been investigated [5,11].

2.2 Double-random-phase encryption

According to the DRPE algorithm [2], a primary image $f(x)$ can turn up to be a noisy-like complex-valued distribution $\psi(x)$ that does not reveal its content, when two random phase masks, $\exp[i2\pi n(x)]$ and $\exp[i2\pi b(\mu)]$ with $n(x)$ and $b(\mu)$ uniformly distributed over $[0,1]$, are used in the spatial and Fourier domains, respectively, as it is mathematically described by

$$\psi(x) = \left\{ f(x) \exp[i2\pi n(x)] \right\} * h(x), \tag{2}$$

where $h(x) = FT^{-1}\left\{\exp\left[i2\pi b(\mu)\right]\right\}$ and FT^{-1} stands for the inverse Fourier transform. Symbol $*$ in Eq. (2) denotes convolution, and coordinates (x) and (μ) correspond to the spatial and frequency domains, respectively, in one-dimensional notation for simplicity.

By multiplying the Fourier transformed encrypted distribution, $FT\left\{\psi(x)\right\}$, by the decryption key, $\exp\left[-i2\pi b(\mu)\right]$, the original primary image can be retrieved provided $f(x)$ is a real and positive function.

Since the introduction of the DRPE algorithm [2], a variety of other proposals based on this encoding technique have been published, leading DRPE and its variants to be one of the most widespread techniques applied in the optical security field (for a review, see for instance, Ref. [12]). In parallel to novel DRPE variant proposals, a number of papers have demonstrated certain vulnerability of the DRPE method due to the fact that is a linear process that facilitates some kinds of attacks [12-14]. DRPE is much more secure when employed in optical systems because it frequently involves some nonlinear effects and additional experimental parameters (optical storage materials, positions, wavelength and polarization of the light beam) that need to be known precisely to retrieve the hidden information. However, since the DRPE can be seen as a cryptographic algorithm that can be alternatively implemented digitally, it is found to be resistant against brute force attacks but vulnerable to known and chosen plaintext and ciphertext attacks [12-14]. For this reason, new methods have been proposed in the last recent years to increase the security of this optical encryption procedure. Among them, the integration of DRPE with photon-counting imaging techniques has been published in 2011 [1].

3. PhCI and DRPE integration

3.1 Two integration procedures

In this Section, two alternative integrating procedures of the photon-counting imaging and the encryption techniques are detailed and compared (Figure 2). The main difference between the two combinations is in the order in which the two techniques are applied. On the one hand, the photon-counting imaging technique is applied to the real-valued primary image $f(x)$. For this approach, marked with (I) PhCI+DRPE in Figure (2), a photon-limited primary image $f_{ph}(x)$ is obtained by applying Eq. (1) to the normalized distribution $g(x)=f(x)\Big/\sum_{j=1}^{M} f(x_j)$. Afterwards, the photon-limited image $f_{ph}(x)$ can be further secured by encrypting this sparse information with the DRPE method (Eq. 2). The decrypted information obtained following such a procedure is named $d_{fph}(x)$. On the other hand, the primary image $f(x)$ is first encrypted using Eq. (2) to produce the distribution $\psi(x)$. In this approach, marked with (II) DRPE+PhCI in Fig. (2), the photon-counting imaging technique is applied to the complex-valued encrypted distribution $\psi(x)$. Taking into account that the encrypted distribution is, in general, of complex nature, both amplitude and phase must be kept for decryption. The photon-counting imaging technique is first applied to the amplitude information, so that it turns to be a binary distribution. Thus, the photon-limited amplitude encrypted distribution, $|\psi_{ph}(x)|$, is generated from the normalized amplitude distribution $g(x)=|\psi(x)|\Big/\sum_{j=1}^{M}|\psi(x_j)|$ using Eq. (1). Only the non-zero amplitude pixels keep the phase information for decryption. The phase information is distributed from 0 to 2π with a resolution of 8 bits at this stage. From the photon-limited amplitude and its

corresponding phase information, a photon-limited encrypted function, $\psi_{ph}(x)$, is obtained and used for decryption. The final decrypted image is called $d_{\psi ph}(x)$.

If one compares the two decrypted images obtained by both procedures (functions $d_{fph}(x)$ and $d_{\psi ph}(x)$ in Figure 3), it is possible to realise that the first one, $d_{fph}(x)$, consists of a sparse distribution of a photon-limited version of the primary image, while the latter, $d_{\psi ph}(x)$, has a noisy-like appearance with higher intensity on average than the former. In both cases, the decoded images hardly resemble the original primary image $f(x)$ and, as a consequence, the text contained in it cannot be recognised. Let us recall, that the integration of PhCI and DRPE is not intended for visualization of the decrypted information, but for verification.

It is worth mentioning the fact that an effective bandwidth reduction can be achieved only from the second integration procedure (II – DRPE+PhCI in Fig. 2) that consists of firstly encrypting the primary image, and secondly obtaining a photon-counting imaging version of the encrypted distribution. In such a case, the reduction in the number of pixels considered in the transmission and decryption processes benefits from the number of photon-counts taken into account in the PhCI technique. The information contained in this sparse representation can be significantly compressed by keeping only the data of the no-null information, similarly to the procedure presented in Ref. [15]. If the first procedure is applied (I – PhCI+DRPE in Fig. 2), the photon-counting imaging technique is used to obtain a photon-limited primary image, and this resulting distribution is then encrypted with DRPE obtaining a non-sparse complex-valued function. In such a situation, no information reduction and therefore, no benefit is achieved in comparison to the DRPE technique.

To authenticate the retrieved signal $d(x)$, which is either $d_{fph}(x)$ or $d_{\psi ph}(x)$, we compare it with the original image $f(x)$ used as a reference, by nonlinear correlation [16]. Nevertheless, a number of other recognition techniques may be used [17-19]. The signals to be compared are Fourier transformed, nonlinearly modified and multiplied in the frequency domain. By inverse Fourier transforming this product, the nonlinear correlation $c(x)$ between both signals is obtained [16]

$$c(x) = FT^{-1}\left\{\left|D(\mu)F(\mu)\right|^{k}\exp\left[i\left(\phi_D(\mu)-\phi_F(\mu)\right)\right]\right\}, \tag{3}$$

where the uppercase denotes Fourier transform of the function in lowercase.

In a k'th-law processor, parameter k defines the strength of the applied nonlinearity. For $k=1$ a linear filtering technique is obtained, whereas $k=0$ leads to a phase extractor that generally enhances the high frequency content. Intermediate values of k permit the features of the processor to be varied. Thus, features such as discrimination capability, noise robustness or peak sharpness can be chosen according to the performance required for a given recognition task [16,20-21]. In this work, we will provide computer simulations to establish the value of parameter k best suited to our verification application. We will analyse the performance of the processor in terms of the discrimination ratio (DR) metrics [18]

$$DR = \left|1-\frac{CC}{AC}\right|, \tag{4}$$

where CC stands for the maximum cross-correlation intensity value of the output correlation plane when a given signal is correlated with the reference primary function, and AC stands for the maximum auto-correlation intensity value obtained when the reference primary image is correlated with itself. This expression can be adapted to the photon-couting imaging technique to deal with large differences in intensity maxima that usually occur. In Eq. (4), as auto-correlation we take AC_{ph}, which is the output

correlation intensity maximum obtained when the primary image $f(x)$ is correlated with $d(x)$, that is the decrypted signal retrieved by any of the integrating procedures described above, either $d_{fph}(x)$ or $d_{\psi ph}(x)$, applied to the authorized primary image. In case of the cross-correlation signal, we consider CC_{ph}, which is the output correlation intensity maximum obtained when the same procedures are applied to the correlation of the primary image $f(x)$ with a different non-authorized primary image, let us denote it by $\tilde{f}(x)$ (Figure 4). A $DR = 0.5$ is chosen as an arbitrary reference to allow a good discrimination between the original and the unauthorized primary images. DR values below the threshold level of 0.5 indicate that the evaluated image is considered as the sought signal, whereas $DR > 0.5$ indicates discrimination of the analysed image from the reference.

3.2 Evaluation results

Figure 3 shows the retrieved images, $d_{fph}(x)$ and $d_{\psi ph}(x)$, obtained using both procedures (I and II of Fig. 2) for photon-counting and encryption integration when the original primary image, $f(x)$, which is the authorized signal, is the input in both processes. A number of photon counts of $N_p = 10^{2.5}$, which corresponds to 0.12% of the image size, is set for the photon limited version of the primary image (procedure I - PhCI+DRPE). For the case of photon limiting the encrypted distribution (procedure II - DRPE+PhCI) $N_p = 10^4$, or equivalently, less than 4% of the image size, is considered. Decoded images are compared to the primary image through nonlinear correlation with $k = 0.3$ and the corresponding intensity autocorrelation outputs are shown in Figure 4. In order to test the discrimination capability of the proposed system, a different but

highly similar text image $\tilde{f}(x)$, which is a non-authorized signal, is used in the described procedures. This text has exactly the same amount of white pixels as the correct primary image (Fig. 4). According to the proposals, function $\tilde{f}(x)$ is either first photon-limited and then encrypted (procedure I – PhCI+DRPE in Fig. 2) or, first encrypted and then photon-limited (procedure II – DRPE+PhCI in Fig. 2), and by using the appropriate decrypting key, the decoded images $\tilde{d}_{fph}(x)$ and $\tilde{d}_{\psi ph}(x)$ are retrieved, respectively. Both decrypted images look like their corresponding counterparts, $d_{fph}(x)$ and $d_{\psi ph}(x)$. Neither the sparse distributions nor the noisy-like images do permit to make out the original text by direct visual inspection in any of the cases. However, we can compare the retrieved images $\tilde{d}_{fph}(x)$ and $\tilde{d}_{\psi ph}(x)$ with the original primary image $f(x)$ through nonlinear correlation to verify their authenticity. The corresponding intensity crosscorrelation outputs are shown in Figure 4 as well. From these results, we can state that even the amount of information kept in the decoded images is insufficient to recognise the original text by the naked eye, it is enough to discriminate between them through optical correlation, as it can be tested from the normalized intensity correlation outputs obtained in this experiment. Only correlation planes corresponding to the authorized primary image contain a high and sharp intensity peak, whereas the correlation planes corresponding to the non-authorized signal provide a low intensity noisy distribution over the whole planes without any remarkable correlation peak. These results are shown as examples of the outputs obtained for the proposed verification system, and they were obtained for a given number of photons on the photon-limited distributions ($N_p = 10^{2.5}$ or equivalently 0.12% of the image pixels for the procedure I - PhCI+DRPE and $N_p = 10^4$ or 3.8% of the image pixels for the procedure II -

DRPE+PhCI) and a particular value of parameter k ($k = 0.3$) that defines the applied nonlinearity in the correlation. We must remark that for the case of applying the photon-counting imaging techniques directly to the primary binary image (procedure I - PhCI+DRPE), it is possible to significantly reduce the number of photons $\left(N_p = 10^{2.5}\right)$, in comparison to procedure II - DRPE+PhCI with the photon-limited version of the encrypted distribution $\left(N_p = 10^4\right)$. For the latter, the random noisy appearance of the encrypted information requires a larger amount of photons to obtain a successful verification of the information. Regarding the possibility of achieving a bandwidth reduction for information transmission, only one procedure permits an effective reduction of the information, which is to consider the photon-limited sparse encrypted distribution, $\psi_{ph}(x)$, of procedure II – DRPE+PhCI (Figure 2). Procedure I – PhCI+DRPE (Fig. 2), which consists of encrypting the photon-limited primary image, $f_{ph}(x)$, contains complex-valued information corresponding to all the pixels of the original primary image. In that sense, no bandwidth reduction is achieved.

To select the most appropriate applied nonlinear correlation, the discrimination ratio was evaluated for several values of parameter k. Figure 5 shows the obtained results for the binary text images, being $f(x)$ the authorized signal and $\tilde{f}(x)$ the non-authorized image, both shown in Fig. 4. The corresponding decrypted signals, $d(x)$ and $\tilde{d}(x)$ respectively, are compared with the original primary image $f(x)$ so that AC_{ph} and CC_{ph} are obtained. Graphs in Fig. 5 depict the mean DR value computed from 20 numerical simulations versus the number of photon counts (N_p). The standard deviation of the whole set of simulations permits to estimate the corresponding error margin. DR values approaching 1 indicate good discrimination between $f(x)$ and

$\tilde{f}(x)$, while DR results close to 0 correspond to recognition of the unauthorized signal as the sought image, thus leading to a wrong verification. Figure 5 also contains a dashed horizontal line corresponding to the established threshold level of $DR = 0.5$. By analysing the results depicted in Figure 5, the number of photons can be more significantly decreased in the case of procedure I - PhCI+DRPE (Fig. 5(a)), limiting the number of photons of the primary image while keeping a satisfactory recognition process. For such a case, higher values of k provide better DR results. However, wider correlation peaks were obtained, making the detection of the sought signal more difficult [1]. A good trade-off between the number of photons and the applied nonlinearity is the pair $N_p = 10^{2.5}$ (0.12%) and $k = 0.3$, for which $DR > 0.7$ is achieved. If we consider the procedure II - DRPE+PhCI (Fig. 5(b)), the reduction of the number of photons is less important than in the previous case, and rather similar performance of the DR is obtained for the tested k values. However, intermediate low values of k are preferable since they provide slightly better DR with sharper and more intense correlation peaks. For this case, $N_p = 10^4$ (3.8%) and $k = 0.3$ were chosen because they have a good recognition result with $DR > 0.8$.

A different type of binary primary image was tested in order to discard a significant influence of the primary image on the verification results. For instance, a dithered natural image was alternatively used in the experiment (Figure 6). The dithered image was built so that its number of white and black pixels strongly matches the binary text and, as a result, they both have approximately the same energy. A non-authorized dithered signal is built by symmetrically rotating the original natural image in the horizontal direction. Both integration approaches were considered. Results for the dithered natural image are shown in Figure 7. As a general rule, results for binary texts and dithered grey level images do not differ qualitatively, and equivalent conclusions

can be extracted from their study. However, it is remarkable that dithered natural images permit a larger reduction on the number of photons while keeping and acceptably good performance in the verification of the information through correlation. For the photon-limited version of the primary image (procedure I - PhCI+DRPE in Fig. 2), $N_p = 10^{1.75}$ (0.02% of image pixels) provides good results, whereas for the photon-limited encrypted distribution (procedure II - DRPE+PhCI in Fig. 2), $N_p = 10^{3.5}$ (1.2%) has a satisfactory performance. Both results correspond to lower photon counts in comparison to the results achieved for the binary text image of Figure 5. According to graphs presented in Fig. 7, and in accordance to Fig. 5, the value of $k = 0.3$ is a good trade-off between DR and peak sharpness and it will be considered for other numerical experiments presented in the paper.

3.3 Phase information compression

Regarding both integrating combinations presented in the paper, procedure II - DRPE+PhCI presents the additional advantage of reducing the amount of information that it is needed to be sent, since the decrypted distribution has a sparse representation that strongly reduces the number of pixels with no-null information. However, taking into account that the encrypted distribution is of complex nature, both amplitude and phase must be kept for decryption. Let us remind that, after applying the photon-counting imaging technique to the encrypted distribution, the amplitude information turns to be a binary distribution, whereas the phase information corresponding to the non-zero amplitude pixels is kept between $[0, 2\pi]$ with its maximum resolution of 8 bits. Further compression can be achieved if we limit the number of bits used for representing the phase information [22-24]. In this work, the limitation of the number of bits is done according to the proposal presented in [24].

Figure 8 shows the verification results in terms of DR for both the binary text and the dithered natural images. Curves depicted in Figure 8 show a similar behaviour except for the case of binary representation of the phase. In general, there is a limiting number of photons N_p for which the two compared images are no longer discriminated. Above this number of pixels, the verification system presents satisfactory results ($N_p = 10^4$ or equivalently 3.8% of the pixels for text image and $N_p = 10^{3.5}$ or 1.2% of the pixels for dithered natural image). Results on the number of photon counts coincide with the ones obtained for 8 bit resolution in previous tests (Fig. 5 and 7) and do not significantly vary when the representation of the phase information is reduced to just 2 bits (or equivalently 4 phase values). For the case of considering just one bit for the reproduction of the phase distribution (that is, 2 phase values) the verification system is not able to discriminate between very similar images, independently of the number of photons.

It is worth to mention that the photon-counting double-random-phase encryption presented in this paper, which allows the verification of the encrypted information and its discrimination from very similar but non-authorized signals, permits a stronger reduction in the number of bits (just 2 bits) in comparison to the results shown in Refs. [22-23]. In these papers, the quality needs in the reconstruction of 3D objects from digital holograms required at least 4-5 bits to obtain an intense correlation peak between the compressed and the uncompressed reconstructed images and about 6-7 bits to visualize a good 3D object reconstruction. The analysis of the results in [22-23] demonstrated that the speckle noise present in the reconstructed objects significantly affected the quality of the retrieved 3D object.

4. Image verification and retrieval

In this test, we combine natural images along with some binary text to build a more general primary image. We want to show the feasibility of the proposed methods to encrypt and verify the information, but also to introduce the possibility of image retrieval from the correlation output result. In such a way, the proposed methods, which were not initially intended for visualization, will also permit information retrieval as other commonly used optical encryption methods.

Images used in the experiment are separately shown in Figure 9. The database consists of three different animal pictures (named A1, A2 and A3) and three different texts (denoted as T1, T2 and T3). Image of the bear (A1) along with the "black-bear" text (T1) on its bottom area is used as primary image. Other images are considered in order to test the discrimination capability of the verification system.

Following the procedures described in Section 3.1, the two approaches for integration of photon-counting imaging and DRPE method are analysed. Firstly, procedure I - PhCI+DRPE (Fig. 2) is applied and a photon-limited version $f_{ph}(x)$ of the primary image $f(x)$ is obtained with $N_p = 10^{3.5}$ (1.2% of pixels). Then, the sparse information is encrypted, $\psi(x)$. By using the appropriate decrypting key, the decoded image $d_{fph}(x)$ is obtained (Figure 10(a)). This decrypted image is compared to all the images of the database (Fig. 9) by nonlinear correlation. According to previous results, parameter k is set to 0.3. Figure 10(b) shows the obtained results. The normalized intensity correlation outputs are shown in the same order of database pictures in Figure 9. Only two intense and sharp peaks point out on the correlation planes obtained for the bear image (A1) and the black-bear text (T1). The location of the peaks corresponds to the center of the objects being correlated as it can be noticed by the axes coordinates. All the other correlation planes have a low intensity noisy background without any

remarkable peak. According to these correlation outputs, taking into account the peak intensity and location, the verification system can also synthesize the retrieved image with the elements of the scene correctly placed to the final user, as depicted in Figure 10(c).

If the second integration approach (procedure II - DRPE+PhCI in Fig. 2) is used, similar results are obtained. Figure 11 shows the obtained results. The primary image $f(x)$ is first encrypted, $\psi(x)$. Photon-counting imaging techniques are applied to the complex-valued encrypted distribution, and function $\psi_{ph}(x)$ is generated with $N_p = 10^{4.5}$ (12% of pixels). By using the correct key, the decrypted image $d_{\psi ph}(x)$ is obtained (Fig. 11(a)). This output is compared to each image of the database through nonlinear correlation with $k = 0.3$. Results are shown in Figure 11(b). From them, only two correlation peaks are obtained for the bear image and text. The other images of the database give low-intensity correlation outputs. These results indicate that the retrieved image consist of two objects of the database centred at the position of the intensity correlation peaks, so it coincides with the image displayed in Figure 10(c).

5. Conclusions

The introduction of photon-counting imaging techniques to encryption algorithms allows the generation of sparse distributions, which may permit bandwidth reduction, and increases the robustness security against intruder attacks.

Two different procedures are considered depending on the order of the application of the two methods to be integrated. First, a photon counting version of a primary image can be obtained prior to its encryption (procedure I - PhCI+DRPE in Fig. 2), or vice versa, a sparse representation of encrypted distribution can be obtained by applying photon-counting imaging (procedure II - DRPE+PhCI in Fig. 2). Both procedures allow

us to increase security of the encryption system against intruders. However, the information in the decoded image is sufficient to verify the primary data by pattern recognition such as nonlinear correlation. In general, the number of photons can be reduced more significantly for the first approach (procedure I - PhCI+DRPE) that is, when a photon-counting version of the primary image is considered, than for the second case (procedure II - DRPE+PhCI) using a photon-counting imaging applied to the encrypted data. However, a substantial and effective bandwidth reduction is only achieved by using the procedure II - DRPE+PhCI. Numerical results are presented for different types of images, such as text or dithered natural images to illustrate the performance of the proposed approaches. Not only has information verification been demonstrated but also retrieval of the original image has been achieved based on the correlation output results.

Acknowledgments

This research work has received financial funding from the Spanish Ministerio de Ciencia e Innovación y Fondo FEDER (project DPI2009-08879).

References

[1] Pérez-Cabré, E., Cho. M., Javidi, B. (2011) "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett., 36 (1), 22-24.

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

[3] Millán, M. S., Pérez-Cabré, E., Javidi, B. (2006) "Multifactor authentication reinforces optical security," Opt. Lett., 31 (6), 721-723.

[4] Pérez-Cabré, E., Millán, M. S., Javidi, B. (2007) "Near infrared multifactor identification tags," Opt. Express, 15 (23), 15615-15627.

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

[6] Goodman, J. W., *Statistical Optics*, John Wiley & Sons, Inc., 2000.

[7] Morris, G. M. (1984) " Scene matching using photon-limited images," J. Opt. Soc. Am. A, 1, 482-488.

[8] Watson, E. A., Morris, G. M. (1992) "Imaging thermal objects with photon-counting detector," Appl. Opt., 31, 4751-4757.

[9] Guillaume, M., Melon, P., Réfrégier, P., Llebaria, A. (1998) "Maximum-likelihood estimation of an astronomical image from a sequence at low photon levels," J. Opt. Soc. Am. A, 15 (11), 2841-2848.

[10] Tavakoli, B., Javidi, B., Watson, E. (2008) "Three dimensional visualization by photon counting computational integral imaging," Opt. Express, 16 (7), 4426-4436.

[11] Cho, M., Mahalanobis, A., Javidi, B. (2011) "3D passive photon counting automatic target recognition using advanced correlation filters," Opt. Lett., 36 (6), 861-863.

[12] Millán, M. S., Pérez-Cabré, E. "Optical data encryption," in *Optical and digital image processing. Fundamentals and applications*, G. Cristóbal, P. Schelkens, H. Thienpont, eds., Wiley-VCH, Germany (2011).

[13] Carnicer, A., Montes-Usategui, M., Arcos, S., Juvells, I. (2005) "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett., 30, 1644-1646.

[14] Frauel, Y., Castro, A., Naughton, T. J., Javidi, B. (2007) "Resistance of the double random phase encryption against various attacks," Opt. Expr., 15, 10253-10265.

[15] Memmolo, P., Paturzo, M., Pelagotti, A., Finizio, A., Ferraro, P., Javidi, B. (2010) “Compression of digital holograms via adaptive-sparse representation,” Opt. Lett., 35, 3883-3885.

[16] Javidi, B. (1989) "Nonlinear joint power spectrum based optical correlation," Appl. Opt., 28, 2358-2367.

[17] Dubois, F. (1993) "Automatic spatial frequency selection algorithm for pattern recognition by correlation," Appl. Opt., 32, 4365-4371.

[18] Sadjadi, F., Javidi, B., *Physics of the automatic target recognition*, Springer, 2007.

[19] Mahalanobis, A. (2009) "Object specific image reconstruction using a compressive sensing architecture for application in surveillance systems," IEEE Trans. AES, 45, 1167-1180.

[20] Millán, M. S., Pérez, E., Chalasinska-Macukow, K (1999) "Pattern recognition with variable discrimination capability by dual non-linear optical correlation," Opt. Commun., 161, 115-122.

[21] Pérez, E., Millán, M. S., Chalasinska-Macukow, K. (2002) "Optical pattern recognition with adjustable sensitivity to shape and texture," Opt. Commun., 202, 239-255.

[22] Naughton, T. J., Frauel, Y., Javidi, B., Tajahuerce, E. (2002) "Compression of digital holograms for three-dimensional object reconstruction and recognition," Appl. Opt., 41, 4124-4132.

[23] Naughton, T. J., McDonald, J. B., Javidi, B. (2003), "Efficient compression of Fresnel fields for Internet transmission of three-dimensional images," Appl. Opt., 42, 4758-4764.

[24] Horrillo, S., Pérez-Cabré, E., Millán, M.S. (2010) "Information compression for remote readable ID tags," J. Opt., 12, 115404.

Figure captions

Figure 1. (a) Primary image $f(x)$ of 512x512 pixel size. (b) Photon-limited versions of $f(x)$ for different photon counts, N_p. The percentage of photons with respect to the original pixel size is given in brackets.

Figure 2. Block diagram of two alternative procedures for combining the photon-counting imaging technique with the encryption method: procedure I - PhCI +DRPE and procedure II - DRPE+PhCI.

Figure 3. (a) Decrypted image $d_{fph}(x)$ retrieved from the encrypted photon-limited primary function with $N_p = 10^{2.5}$ (0.12%). (b) Decrypted image $d_{\psi ph}(x)$ obtained from the photon-limited encrypted distribution with $N_p = 10^4$ (3.8%).

Figure 4. Intensity correlation outputs for binary texts used as authorized $f(x)$ and non-authorized $\tilde{f}(x)$ signals. Both procedures for integrating photon counting imaging techniques and DRPE method are applied. The I - PhCI+DRPE procedure is obtained with $N_p = 10^{2.5}$ (0.12%) and $k = 0.3$. The II - DRPE+PhCI approach is applied with $N_p = 10^4$ (3.8%) and $k = 0.3$.

Figure 5. DR versus N_p for the results corresponding to the primary binary text. Different values of k are analyzed for the nonlinear correlation. Integration procedure considers: (a) I – PhCI+DRPE; and (b) II – DRPE+PhCI.

Figure 6. Top: Dithered natural image used for the experiments. Bottom: (left) An enlarged area of the original grey level picture, (Right) the same area of the dithered version.

Figure 7. DR versus N_p for the results corresponding to the primary dithered natural image. Different values of k are analyzed for the nonlinear correlation. Integration procedure considers: (a) I – PhCI+DRPE; and (b) II – DRPE+PhCI.

Figure 8. DR versus N_p for (a) binary and (b) natural primary images. Nonlinear correlation with $k = 0.3$ is applied. Different number of phase values (PV) is considered for the reproduction of the phase information of the photon-limited version of the encrypted distribution. Integration procedure considers II – DRPE+PhCI.

Figure 9. Database used in the work for information verification and image retrieval. Picture A1 along with text T1 are combined to built the primary image for the experiment.

Figure 10. (a) Decrypted image $d_{fph}(x)$ with $N_p = 10^{3.5}$ (1.2% of the image pixels). (b) Intensity correlation outputs when Fig. 10(a) is nonlinearly correlated ($k = 0.3$) with the whole database (Fig. 9). (c) Retrieved image corresponding to the correlation peak intensity and location obtained in (b).

Figure 11. (a) Decrypted image $d_{\psi ph}(x)$ with $N_p = 10^{4.5}$ (12% of the image pixels). (b) Intensity correlation outputs when Fig. 11(a) is nonlinearly correlated ($k = 0.3$) with the whole database (Fig. 9).

Figure 1 (a)

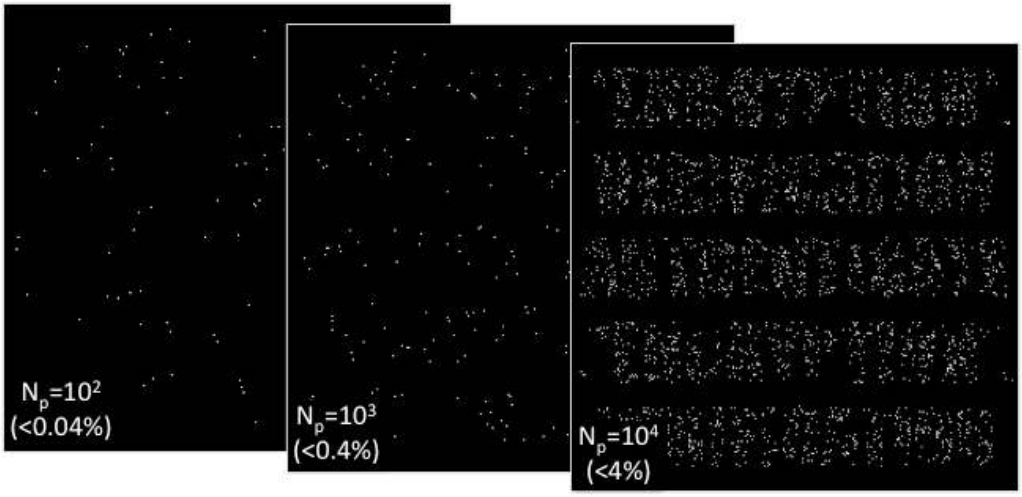

Figure 1 (b)

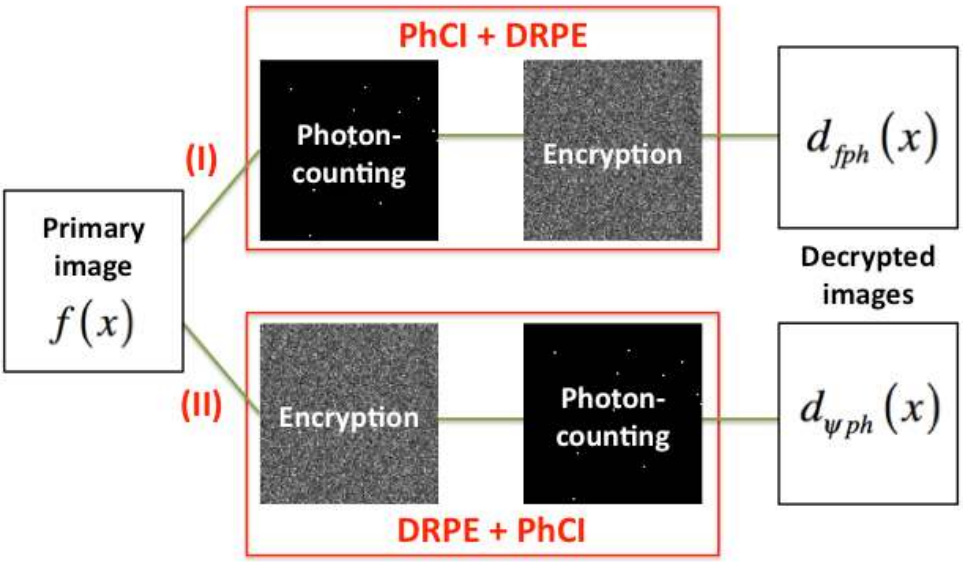
PhCI + DRPE
Photon-counting
Encryption
$d_{fph}(x)$
(I)
Primary image
$f(x)$
Decrypted images
(II)
Encryption
Photon-counting
$d_{\psi ph}(x)$
DRPE + PhCI

Figure 2

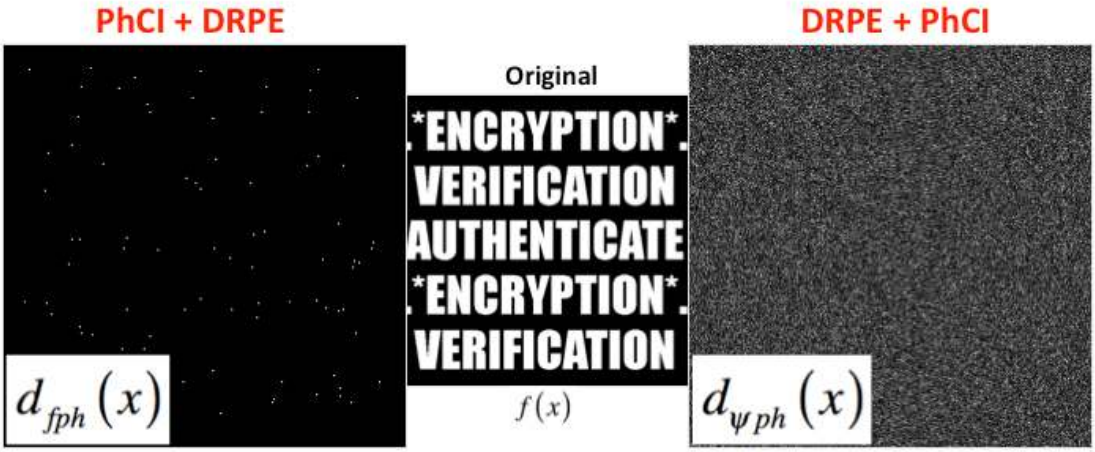
PhCI + DRPE
DRPE + PhCI
Original
ENCRYPTION.
VERIFICATION
AUTHENTICATE
ENCRYPTION.
VERIFICATION
$d_{fph}(x)$
$f(x)$
$d_{\psi ph}(x)$
(a)
(b)

Figure 3

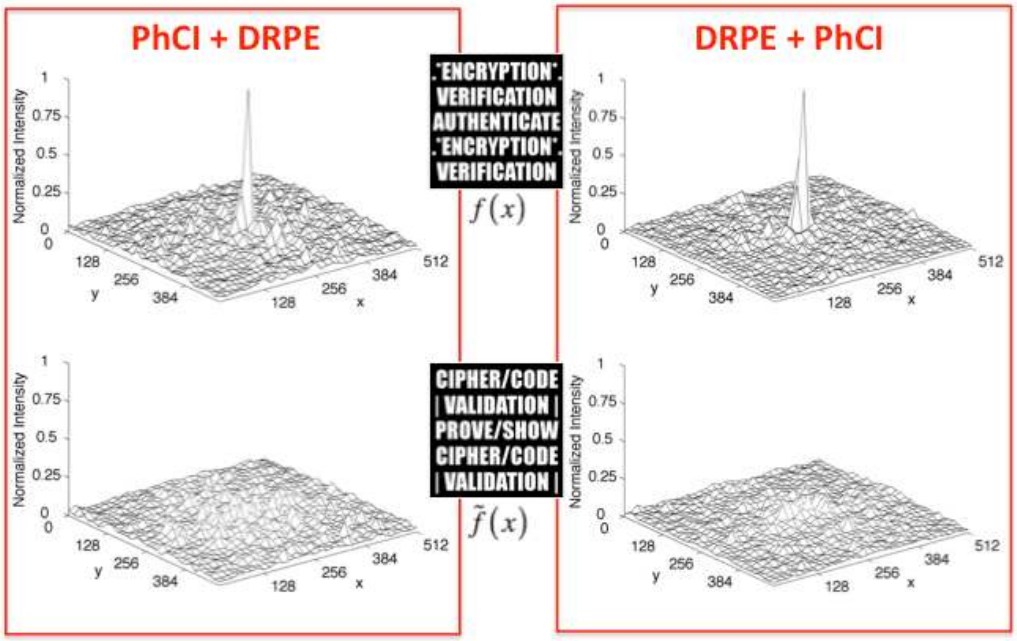
PhCI + DRPE
DRPE + PhCI
"ENCRYPTION"
VERIFICATION
AUTHENTICATE
"ENCRYPTION"
VERIFICATION
$f(x)$
CIPHER/CODE
| VALIDATION |
PROVE/SHOW
CIPHER/CODE
| VALIDATION |
$\tilde{f}(x)$
Normalized Intensity
0
0.25
0.5
0.75
1
128
256
384
512
x
y

Figure 4

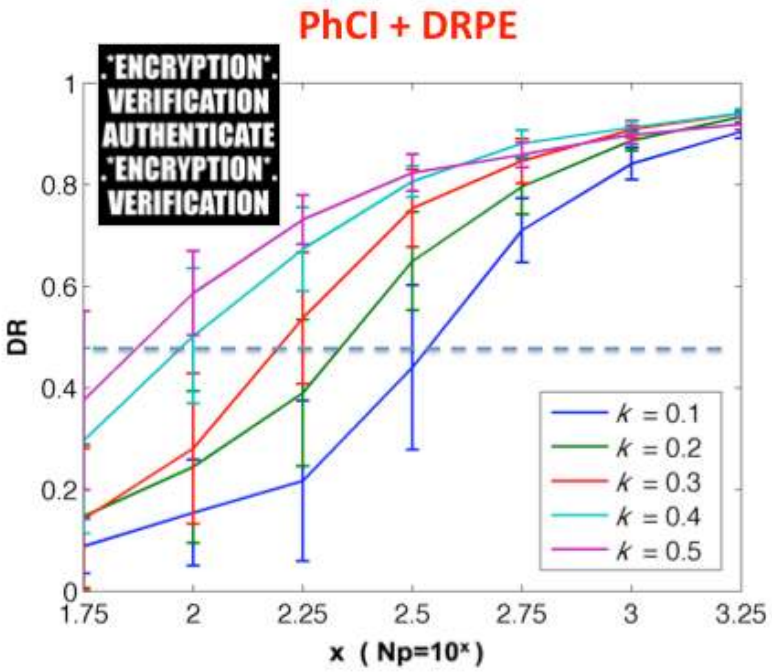

Figure 5 (a)

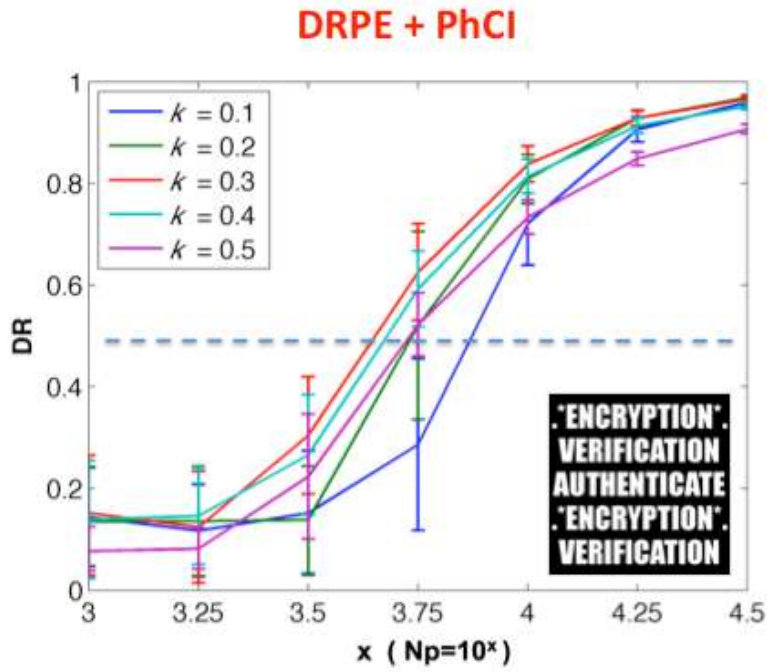

Figure 5 (b)

Figure 6

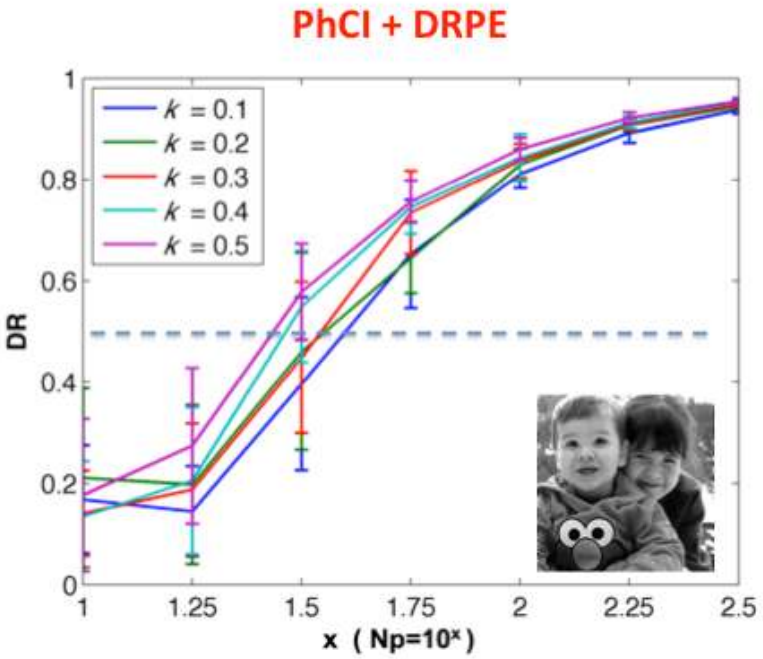

Figure 7 (a)

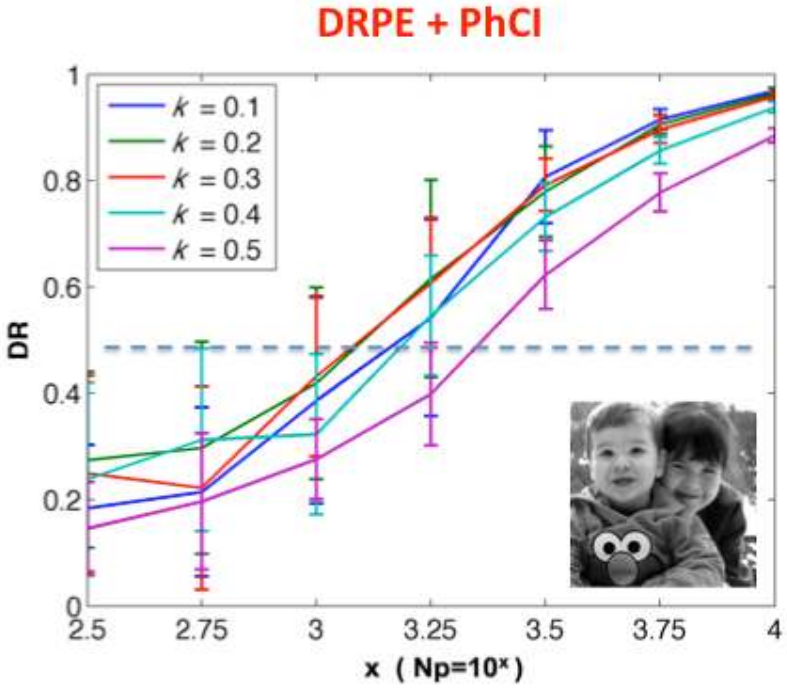

Figure 7 (b)

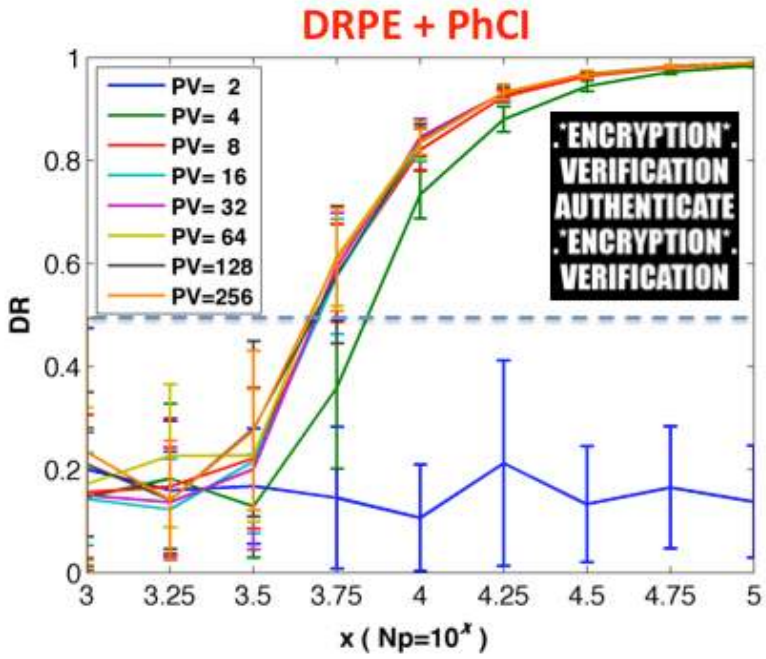

Figure 8 (a)

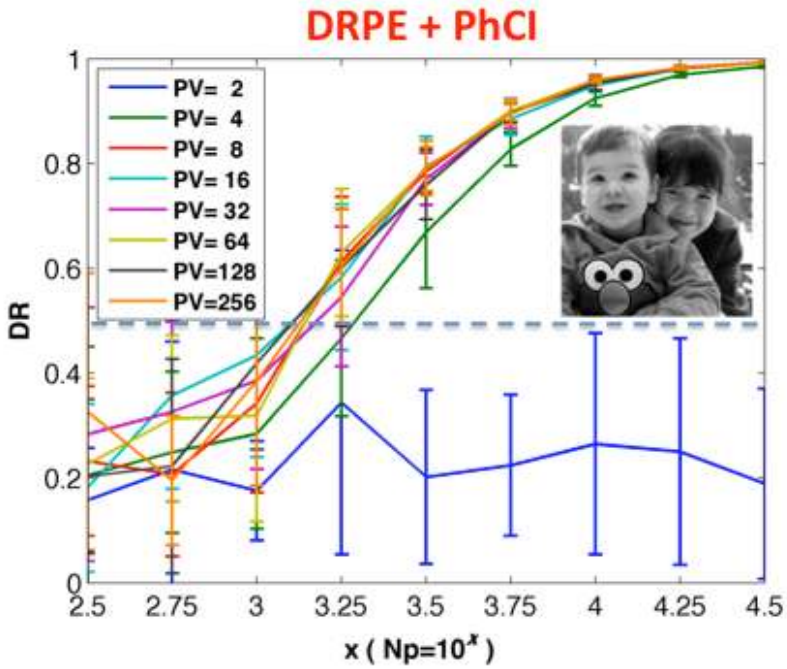

Figure 8 (b)

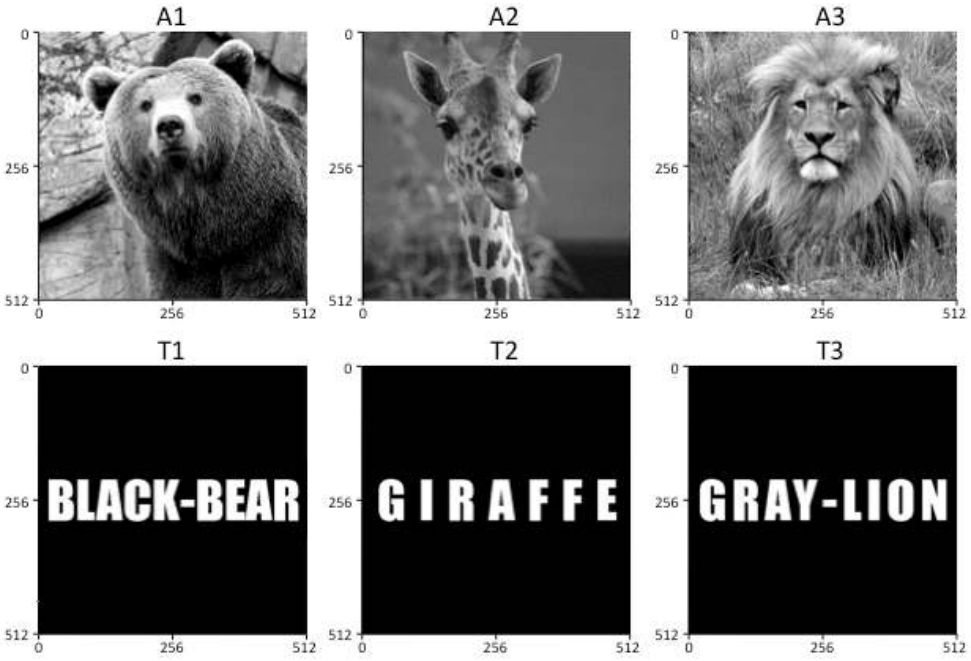

Figure 9

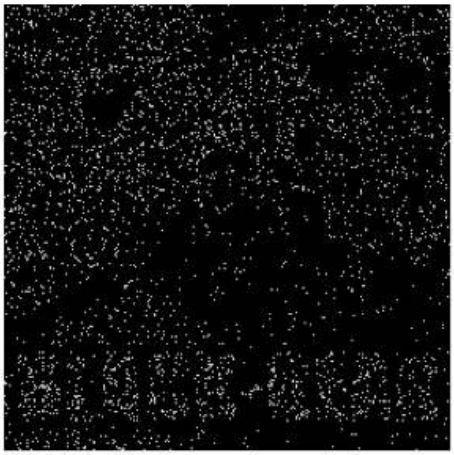

Figure 10 (a)

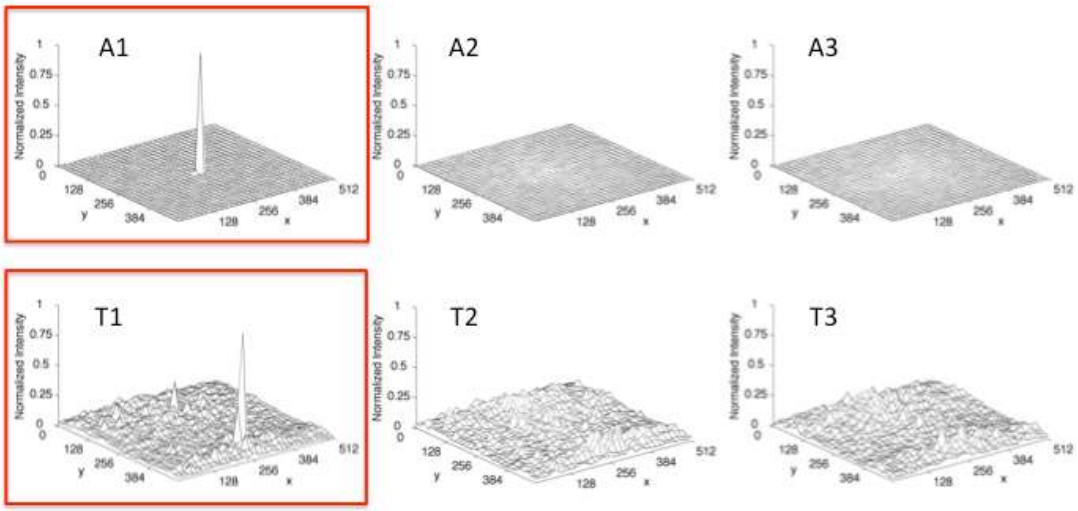

Figure 10 (b)

Figure 10 (c)

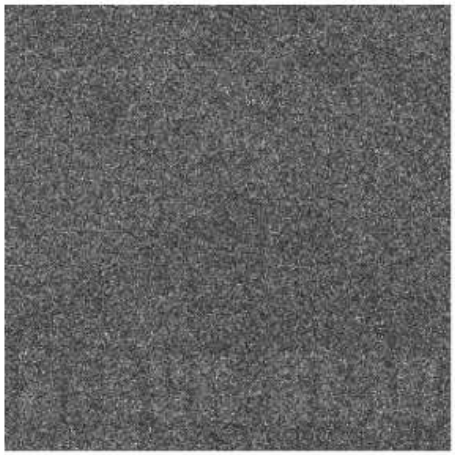

Figure 11 (a)

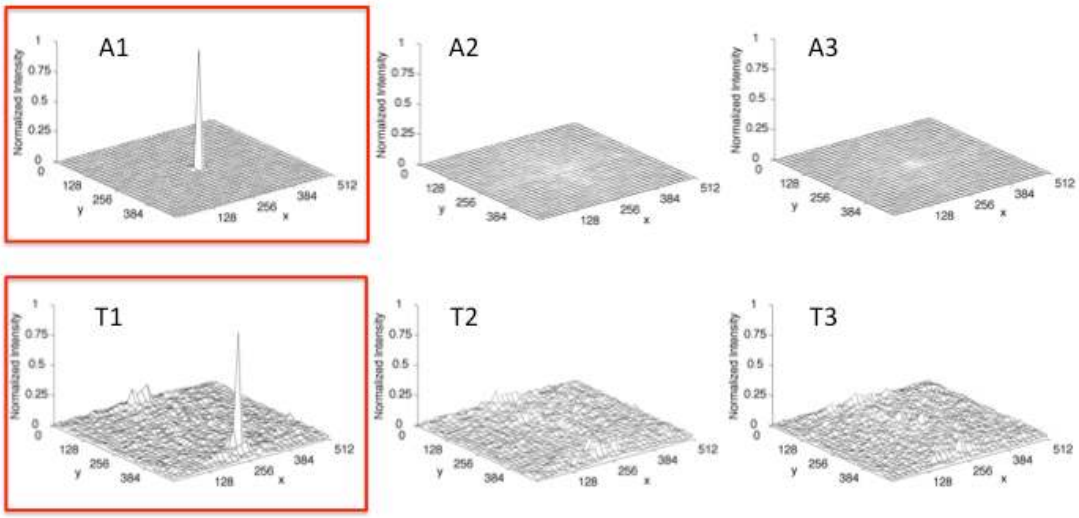

Figure 11 (b)