Role of phase key in the double random phase encoding technique: an error analysis

David S. Monaghan,[1] Guohai Situ,[2] Unnikrishnan Gopinathan,[2]
Thomas J. Naughton,[3] and John T. Sheridan[1,*]

[1]School of Electrical, Electronic and Mechanical Engineering, College of Engineering, Mathematics and Physical Sciences, Optoelectronic Research Centre, the SFI-Strategic Research Cluster in Solar Energy Conversion, University College Dublin, Belfield, Dublin 4, Ireland

[2]Institut für Technische Optik, Universität Stuttgart, Pfaffenwaldring 9, 70569 Stuttgart, Germany.

[3]Department of Computer Science, National University of Ireland, Maynooth, Ireland, and University of Oulu, RFMedia Laboratory, Oulu Southern Institute, Vierimaantie 5, 84100 Ylivieska, Finland (tomn@cs.nuim.ie)

*Corresponding author: e-mail: john.sheridan@ucd.ie

Received 13 February 2008; revised 9 June 2008; accepted 23 June 2008;
posted 24 June 2008 (Doc. ID 92751); published 15 July 2008

We perform a numerical analysis of the double random phase encryption–decryption technique to determine how, in the case of both amplitude and phase encoding, the two decryption keys (the image- and Fourier-plane keys) affect the output gray-scale image when they are in error. We perform perfect encryption and imperfect decryption. We introduce errors into the decrypting keys that correspond to the use of random distributions of incorrect pixel values. We quantify the effects that increasing amounts of error in the image-plane key, the Fourier-plane key, and both keys simultaneously have on the decrypted image. Quantization effects are also examined. © 2008 Optical Society of America

OCIS codes: 200.4740, 100.2000, 070.2580, 000.4430.

1. Introduction

Optical encryption has the potential to offer high-speed parallel encryption of 2D image data. Double random phase encryption [1] (DRPE) is an optical-image encryption technique that involves the use of two random phase keys, one placed in the input domain and one placed in the Fourier domain. If these random phase keys are generated by using statistically independent white noise, then the encrypted image is also a stationary white noise. Since its introduction in 1995, DRPE has generated much interest and has been the focus of many studies [2–7]. One of the major advantages of DRPE is that it has an optical implementation; see Fig. 1. The physical implementation of such an optical system gives rise to many practical issues; however a thorough numerical analysis of DRPE is extremely important if it is to be used as an encryption system.

There are two primary modes of operation of the DRPE technique, which depend on the form of the data to be encrypted:

1. Amplitude encoding (AE), with a gray-scale input image, and
2. Phase encoding (PE), in which throughout this paper we assume that only the input field phase is modulated.

While the optical systems used to encrypt the data in both cases are very similar, there are significant differences in the decryption, analysis, and breaking of these encoding systems. Figure 2 shows a block diagram explaining the encryption and decryption process for both AE and PE and is referred to throughout this paper.

In a physical implementation of both the AE and PE optical encryption systems it is necessary to

0003-6935/08/213808-09$15.00/0

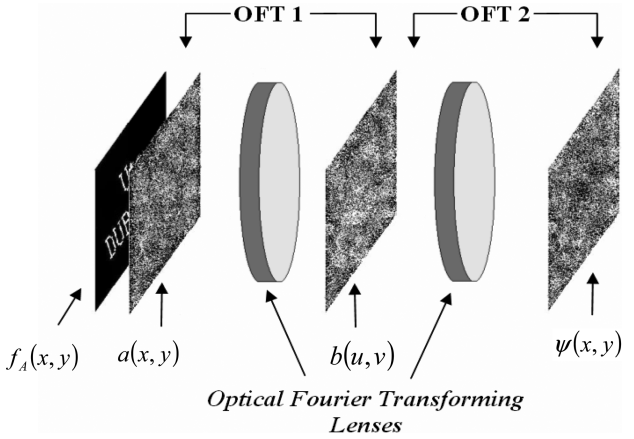

Fig. 1. Possible optical implementation of DRPE. OFT, optical fourier transform. $f_A(x,y)$ is the input image, $a(x,y)$ and $b(u,v)$ are the phase keys, and $\Psi(x,y)$ is the encrypted output image.

capture the phase information of the encrypted field. Since (CCD) cameras can only capture the intensity of a wave field, digital holographic techniques [8–10] must be employed to extract the full complex wave field information. However, when an AE input image has been encrypted using the DRPE technique, knowledge of the image-plane phase key, $a(x,y)$, is not necessary when the decryption process is carried out . This is because, in this case, only the intensity of the input image is required, and therefore the phase in the output decrypted image contains no useful information and is unnecessary, i.e., $|e^{j2\pi a(x,y)}|^2 = 1$.

When a PE input image (phase data) is used, both the image- and the Fourier-plane keys, $a(x,y)$ and $b(u,v)$, are required in the decryption process. This

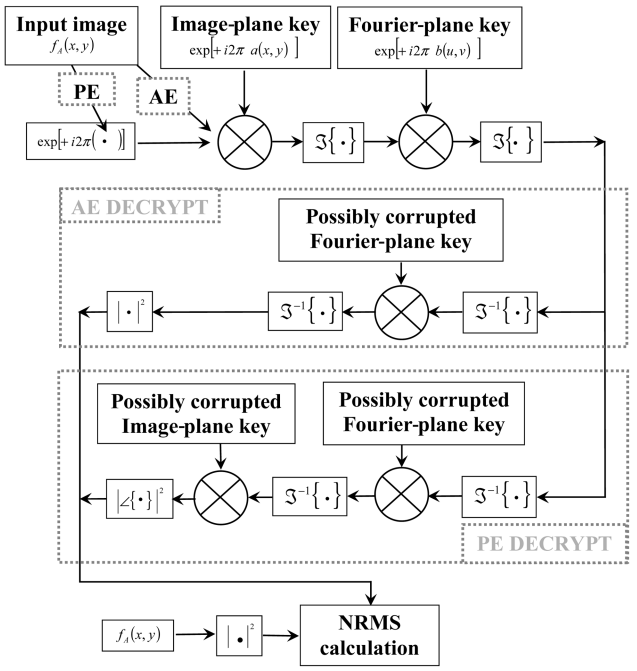

Fig. 2. Block diagram of the similar encryption processes for AE and PE and the different decryption processes that lead to an NRMS value for a decrypted image.

would imply that the attackers job is more difficult, as in the PE case they have to find two phase keys, $a(x,y)$ and $b(u,v)$, in order to break the system, as opposed to needing to find only one, $b(u,v)$, for the AE case.

Should the attacker have access to a cipher–text pair, it has already been shown that in the case of AE heuristic methods [6] can be used to extract the DRPE Fourier key, $b(u,v)$, with a normalized root mean square (NRMS) technique error below 10% within a reasonable amount of time, i.e., within less than an hour using a personal computer. Other methods can be used if several cipher–text pairs are available when the system is attacked, and such techniques have been found to be very effective [11,12].

In this paper we exam the sensitivity of the DRPE technique to errors in the key(s) used for decryption in both the AE and PE cases. Specifically we wish to know if both keys are as significant as each other, or whether the accuracy of one is more important than the other. If the accuracy of one key were less important than the other, then the time required to find an acceptably good approximation to that key, using a heuristic approach, would be greatly decreased. Clearly the informed attacker will apply effort appropriately to the key of greater significance. A further aim in this paper is to examine the type and quantity of noise in the decrypted outputs that is due to random errors in the keys with the hope of developing strategies for attacking such techniques.

To quantify the relative effects of errors in the pixel values, which we introduce in the image- and Fourier-plane keys $a(x,y)$ and $b(u,v)$, we examine the resulting errors in the decrypted images. We compare the errors in the decrypted data resulting from both keys' having identical error properties simultaneously as well as the effect of similar error levels in the two keys individually. The resulting decrypted images are examined for a range of error levels.

In all of the results presented here the encryption process is performed error free, and then errors are introduced by us into the phase keys during the decryption process. Therefore we numerically examine the effect on the decrypted image of errors introduced in the decryption keys. In this study we assume perfect encryption in all cases. In this paper, while we have examined several gray-scale images, the representative results were produced exclusively by using the Lena image [13].

This paper is organized in the following way. In Section 2 we discuss the error metric we have chosen to use to evaluate the DRPE technique and indicate how it is applied in this paper to provide a meaningful comparison between the AE and PE cases. In Section 3 we explain the two encoding procedures under study here, AE and PE. In Section 4 the results for both the AE and PE cases are given. The effect of degrading the quantization of the decryption keys is

also discussed, and a brief conclusion is presented in Section 5.

2. Error Metric

The metric we use to quantify the amount of error in an incorrectly decrypted image is the normalized root mean squared (NRMS) error. This compares an incorrectly decrypted image with the original input image and is calculated as follows:

$$\mathrm{NRMS} = \sqrt{\left(\sum_{i=1}^{N}\sum_{j=1}^{N}|I_d(i,j) - I(i,j)|^2\right)} \Big/ \sqrt{\left(\sum_{i=1}^{N}\sum_{j=1}^{N}|I(i,j)|^2\right)}. \quad (1)$$

In this equation $I_d(\cdot)$ and $I(\cdot)$ represent the intensities of the decrypted and original images, respectively. We note that the NRMS is positive valued and that when NRMS $= 0$ perfect (error free) decryption has taken place.

In all of the examples presented in this paper the encryption–decryption process is performed numerically by using a standard fast Fourier transform algorithm [14]. Each data pixel is represented by a single complex value in a finite 2D array in the computer. Thus we neglect all physical modeling issues, e.g., spatial light modulator fill factor, polarization, and diffraction effects [15,16]. Such simplifications are tolerated only because it is an examination of the nature of the DRPE technique, which is our primary consideration here, and not the nonideality introduced by the physical limitations of the optical system implementation.

In the case of AE the comparison of the input and decrypted gray-scale images is straightforward by using the NRMS, Eq (1). However in the case of PE the input data is contained in the phase information (we assume no amplitude variation). To calculate the NRMS the output phase image is converted to a normalized amplitude image, where the range $[0, 2\pi]$ is mapped to the range $[0, 1]$. In this way a comparison of the AE and PE results can be made.

In both the AE and the PE case we add the error to the decryption keys in the same manner. We first select a pixel coordinate in the phase key plane, which is denoted either (x,y) in the image plane or (u,v) in the Fourier plane. The value of these coordinates are assigned by using the Matlab `rand` function [14]. The `rand` function returns a pseudorandom number uniformly distributed in the interval $(0, 1)$ and is based on a 35-element vector that dictates the current state of the uniform generator. By setting the state of the random number generator to a starting position that is based on the current time and date, we can ensure that it will provide us with a different pseudorandom sequence for every run. Once the pixel coordinate has been selected, we assign it a quantized phase value, using the same random number generator to select the quantized value, using a modified, evenly weighted, roulette algorithm to select a phase value from the set of all possible quantized phase values for the phase keys.

It should be noted that other error metrics exist that can be used to provide estimates of the effects of noise and key error [4]. The NRMS error metric, as defined in Eq (1), provides a direct measure of the Euclidean distances between intensity images. Since it is the intensity of the decrypted data that is the quantity of primary interest, and since it is intensity values that are measured during experiments, we believe that the NRMS provides useful insights. However, it should be emphasized that all the conclusions presented in this paper regarding the relative performance of the AE and PE cases are based on comparison of the two methods by using the NRMS metric.

3. Encoding Procedure

A. Amplitude Encoding

As stated, Fig. 1 shows a possible optical implementation of the DRPE technique. In an AE setup we denote the input amplitude image by using $f_A(x,y)$, where x and y are the spatial coordinates and the subscript A indicates that the input is a gray-scale amplitude image. The image is first normalized and then multiplied by the image-plane phase mask, $R1 \sim \exp[+i2\pi a(x,y)]$, and the resultant wavefront is Fourier transformed and then multiplied by the second phase mask, $R2 \sim \exp[+i2\pi b(u,v)]$. The second Fourier transform is then performed to give the encrypted image, denoted Ψ. Therefore in the AE case a perfectly encrypted image is given by

$$\Psi(x,y) = \mathfrak{F}\{\mathfrak{F}\{f_A(x,y)\exp[+i2\pi a(x,y)]\} \times \exp[+i2\pi b(u,v)]\}. \quad (2)$$

The perfect AE decryption process follows from Eq. (2) and is given by

$$f_A(x,y) = \mathfrak{F}^{-1}\{\mathfrak{F}^{-1}\{\Psi(x,y)\}\exp[-i2\pi b(u,v)]\} \times \exp[-i2\pi a(x,y)]. \quad (3)$$

Both processes (encryption and decryption) are illustrated in Fig. 2. We analyze the behavior for the AE case by perturbing the Fourier-plane phase key, $b(u,v)$, used in the decryption process.

Perturbation studies have been carried out in the past [17] in which the robustness of the decryption process is scrutinized to see how a perturbation of the coded image modifies the resulting decoded image. In this study we assume that the coded image is produced by following a perfect encryption process, i.e., without the presence of noise, and we study the effects on the decoded image arising owing to incorrect pixel values in the decrypting phase keys.

In this AE case we move away from a perfect Fourier-plane phase key, $b(u,v)$, by randomly select-

ing an increasing number of pixel locations in the key and assigning them, with uniform probability, a randomly quantized phase value. Using this approach we examine how this process leads to error accumulation in the decrypted image. In Fig. 3 we plot the NRMS errors in the decrypted image on the vertical axis, for the AE case (triangles), and as a function of the percentage of incorrect pixels on the horizontal axis. As discussed, for the AE case $a(x,y)$ is unnecessary to the decryption process; see Fig. 2.

In a brute-force or known plaintext–ciphertext attack, the attacker could use the NRMS as a metric indicating the quality of the estimated key. The NRMS curve in Fig. 3 allows us to simulate an attacker who has *a priori* knowledge of the AE system, i.e., who knows the number of pixels in the key and the quantization levels and who applies the NRMS to search for the decrypting phase key $b(u,v)$ by using heuristic or other approaches. Thus the AE result presented in Fig. 3 indicates the robustness of the DRPE technique to such attacks. So, if a phase key could be obtained with a known number of correct pixel values, the graph would indicate what level of NRMS error it would produce. The opposite, however, does not hold true, but this, as yet, cannot be proved. For example, if a phase key that produced a known NRMS value is obtained, the number of correct pixels in that key cannot be ascertained from the graph in Fig. 3. To be certain of this, the entire key space would need to be mapped, and since the key space for this case contains $16^{65,536}$ possible keys (16 quantization levels and $256 \times 256 = 65,536$ pixels), checking each one is not feasible.

B. Phase-Encoding

In this case the input Lena image, $f_A(x,y)$, is encoded as a phase image where the normalized amplitude in the range $[0,1]$ is mapped to the range $[0,2\pi]$ and is denoted

$$f_P(x,y) = \exp[+i2\pi f_A(x,y)], \tag{4}$$

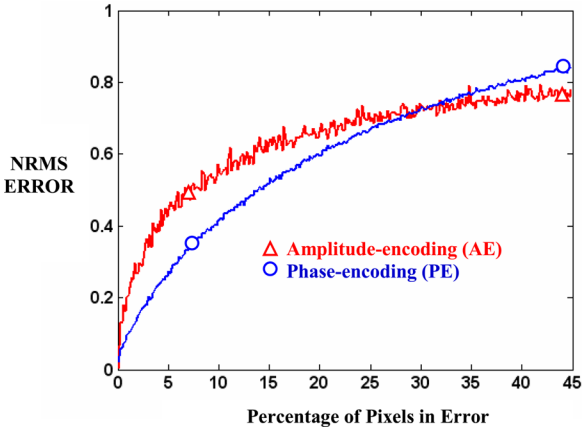

Fig. 3. (Color online) AE compared with PE. The horizontal axis shows the percentage of pixels that are in error in the Fourier-plane key, $b(u,v)$. The vertical axis shows the NRMS error as described in Section 2. With NRMS = 0 the decryption is perfect.

where the subscript P indicates that the image is a phase image. The encryption and decryption processes are the same as described above; however Eqs. (2) and (3) are rewritten as follows:

$$\Psi(x,y) = \mathfrak{F}\{\mathfrak{F}\{\exp[+i2\pi f_A(x,y)]\exp[+i2\pi a(x,y)]\} \times \exp[+i2\pi b(u,v)]\}, \tag{5}$$

$$|f_P(x,y)| = |\mathrm{Arg}(\mathfrak{F}^{-1}\{\mathfrak{F}^{-1}\{\Psi(x,y)\}\exp[-i2\pi b(x,y)]\} \times \exp[-2\pi a(u,v)])|, \tag{6}$$

respectively. As in the AE case, the Fourier-plane phase key $b(u,v)$ is perturbed by an increasing amount, and the resulting error is quantified. In this case $a(x,y)$ is first assumed to be exactly known, i.e., to contain no errors, and it is necessary in the decryption process; see Fig. 2. Below the PE case in which both decrypting keys are perturbed is also examined.

4. Results

A. Amplitude Encoding and Phase-Encoding Results

The standard test image used for all the simulation presented in this paper is the 256×256 pixel grayscale Lena image [13]. Figure 3 contains a second curve plotted for the PE case (circles). The percentage of pixels that are in error is noted on the horizontal axis, and the resulting NRMS error is indicated on the vertical axis. This graph indicates that as the number of incorrect pixels in the $b(u,v)$ Fourier-plane phase key starts to increase, the AE case performs better than the corresponding PE case. This is based on the observation that a small number of incorrect pixels in the $b(u,v)$ phase key will, in general, produce a higher NRMS error in the AE case than in the PE case. Thus the PE case is more robust (less sensitive) to incorrect pixel values in $b(u,v)$, which may simplify the task of any potential attacker in finding an acceptable estimate of $b(u,v)$.

As previously noted, in the PE case it is necessary to know both the image-plane phase key $a(x,y)$ and the Fourier-plane phase key $b(u,v)$ in order to decrypt $\Psi(x,y)$, whereas in the AE case $a(x,y)$ is not required in the decryption process, as only the intensity of the output image contains the encrypted information; see Fig. 2. Hence in the PE case both encryption keys are needed for decryption, which increases the complexity of breaking the system. The question therefore arises as to how errors in the two keys, $a(x,y)$ and $b(u,v)$, effect the NRMS error values.

What we have found is that errors in the two keys affect the output image differently. Figure 4 contains the two previous curves from Fig. 3 but also contains two additional curves. As indicated, the two curves reproduced from Fig. 3 assume that the image-plane phase key $a(x,y)$ is either fully known or not necessary. The two extra curves are formed when (i) the Fourier-plane phase key $b(u,v)$ is assumed to be fully

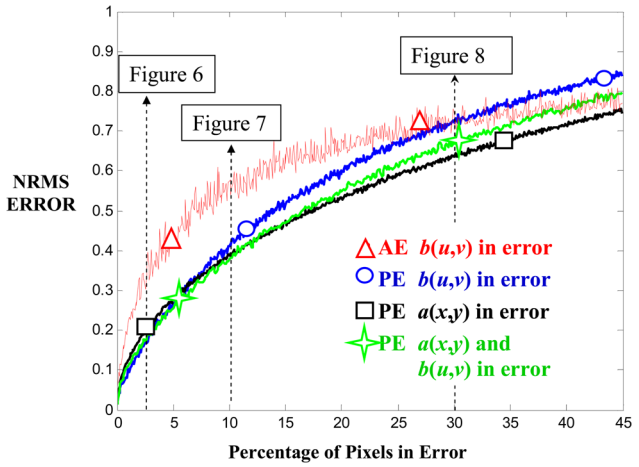

Fig. 4. (Color online) The curve marked by the triangle represents AE. The other three curves look at PE for the cases when the phase keys, $a(x,y)$ and $b(u,v)$, are in error separately and at the same time. The dashed lines refer to Figs. 6–8, which show examples of output images at these error levels.

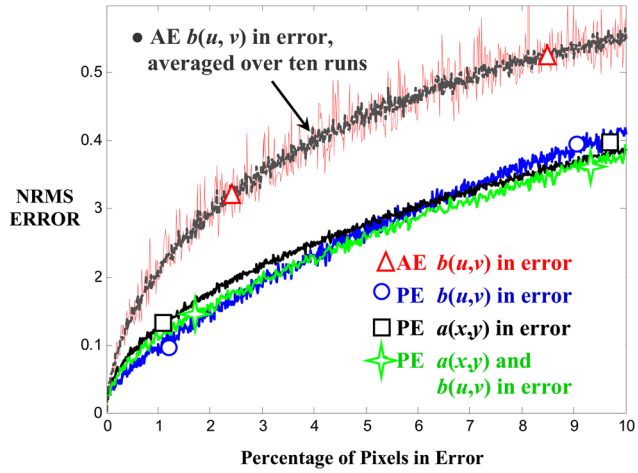

Fig. 5. (Color online) Enlarged graph of a portion of Fig. 4; note the scale on the axes. Superimposed on the AE case is the curve that shows the results for ten runs by using different phase keys and is then averaged (grey dots).

known and $a(x,y)$ is randomly perturbed (squares); and when (ii) both of the phase keys are perturbed, as described below (stars). From the graph the results suggest that the Fourier-plane phase key, $a(x,y)$, is more sensitive to incorrect pixel values than the image-plane phase key, $b(u,v)$, and generates a larger NRMS value for weak perturbations, i.e., low error levels.

To allow a meaningful comparison between the situations when a single key and when both phase-keys are perturbed, an equal number of pixels are always randomized. Thus, when on the graph it indicates that, for example, 20% of the pixels are incorrect, this means that either 20% of the pixels in a single key are in error or that 10% of the pixels in both keys are simultaneously incorrect; therefore the total amount of error is consistently defined in all cases.

Figure 5 provides an enlarged version of Fig. 4 close to the origin; note the scale on the horizontal axis. As before, this graph indicates that for a lower number of pixels in error the PE cases are less sensitive than the equivalent AE case to the combined effects of the same number of incorrect pixel values equally distributed between the two phase keys. We can deduce from the three different PE cases examined that as the percentage of incorrect pixels increases it is more important to have the Fourier-plane phase key, $b(u,v)$, as correct as possible. This is implied, as both of the other cases are less sensitive to incorrect pixel values. In Figure 5 we also have superimposed an average AE curve. To generate this curve the simulation was run ten times, using different random phase keys, and the results averaged. Examining Fig. 5, we note that averaging over ten results merely smooths out the curve but does not alter the slopes or trends observable in the graph. Similar results were observed for each of the PE cases but are not shown in the graph to avoid overcrowding.

Figures 6–8 show decryptions of Lena for the AE case and for all three of the PE cases examined. These images are decrypted at three levels of incorrect pixels, 2.5%, 10%, and 30%. In Figure 4 the level at which these images are taken is indicated by the vertical dashed lines. In these images it can be seen that there are two distinct types of noise. One of these is "salt and pepper" type noise and can be easily removed with median filtering; see Figs. 6(c), 7(c), and 8(c). The other is Gaussian noise and is more difficult to remove [18]; see Figs. 6(a), 7(a), and 8(a). Both of these types of noise are present in Figs. 6(b), 6(d), 7(b), 7(d), 8(b), and 8(d). Therefore by strategically postprocessing these images the image quality in the PE cases can be improved. It should be noted that even when the NRMS error in an output image is very high, greater than 0.7 NRMS, it is still clearly possible to recognize, by eye, that the image is that of a human head.

B. Quantization Effects

Quantization effects are important to understand from a number of perspectives. In the context of attacks on the DRPE, an attacker may not know the correct quantization levels being used. Furthermore, as we have demonstrated, an attacker may deliberately choose a lower quantization level to expedite the breaking of the encryption technique without too great an NRMS penalty. If the DRPE becomes widely used, it will not be possible to guarantee that all optical encryption users will have access to the highest-quality equipment, and indeed some users may choose different equipment to trade-off speed for reliability. Finally, the resolvability of quantization levels will ultimately be related to robustness against noise and thus to the operational signal-to-noise ratio within the system.

In this section we proceed by simulating the affect of quantization on the phase keys for the AE case and the three PE cases. We perform perfect encryption as

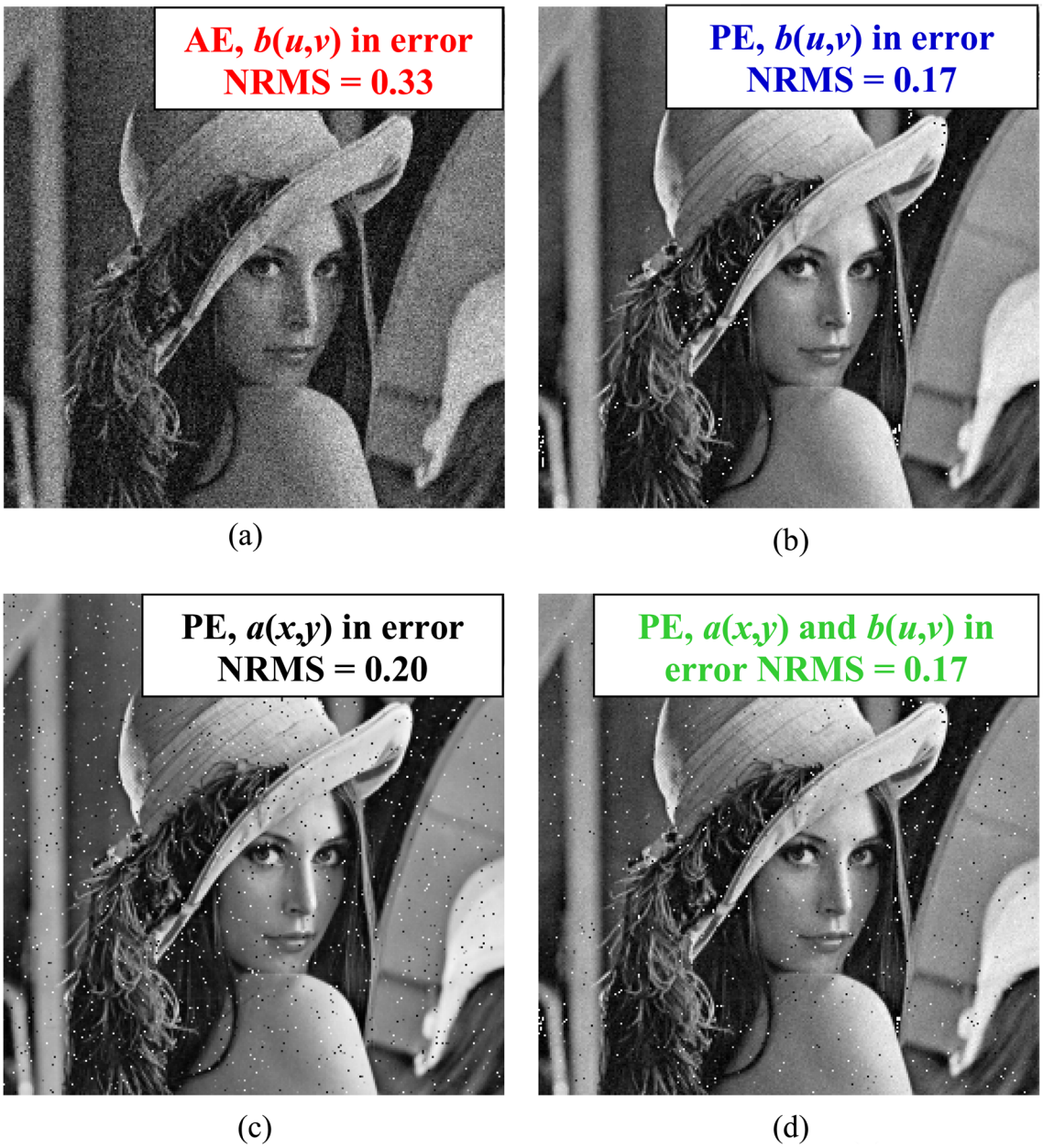

Fig. 6. (Color online) Results when 2.59% of phase key pixels are in error. (a) AE case with $R2$ in error and NRMS ~ 0.33. (b)–(d) PE case with a NRMS of (b) 0.17, (c) 0.20, and (d) 0.17. In (b) $R2$ is in error. In (c) $R1$ is in error, and in (d) both $R1$ and $R2$ are in error.

in the previous cases and introduce errors into the decrypting phase keys. If we assume that we start with two 8 bit phase keys, each with 256 quantization levels, we requantize the decrypting phase keys for lower quantization levels and then calculate the resultant NRMS error. Figure 9 shows three curves for the three PE cases. The number of bits used in both decrypting phase keys is indicated along the horizontal axis, and the NRMS error is given on the vertical axis. For the two cases in which only one of the phase keys is in error, the other is assumed to remain unchanged from the original 8 bit key. In the case where both phase keys are in error the total number of bits is shared between the two phase keys. In the first two cases this means that one phase key uses 8 bits and the phase key in error uses only 4. However, in the third case when both are in error this means that both of the phase keys are in error and use an equal number of bits. For example when the horizontal axis indicates that there are 12 bits being used, the two keys use 6 bits each. In the case where both keys are being requantized, the NRMS error values for the odd points (15, 13, 11, etc.) on the horizontal axis of the graph are estimated by interpolation between the two adjacent even values.

The AE case is also examined in Fig. 9, and although the image-plane phase key is not necessary for decryption, it is still assumed to have 8 bits. So

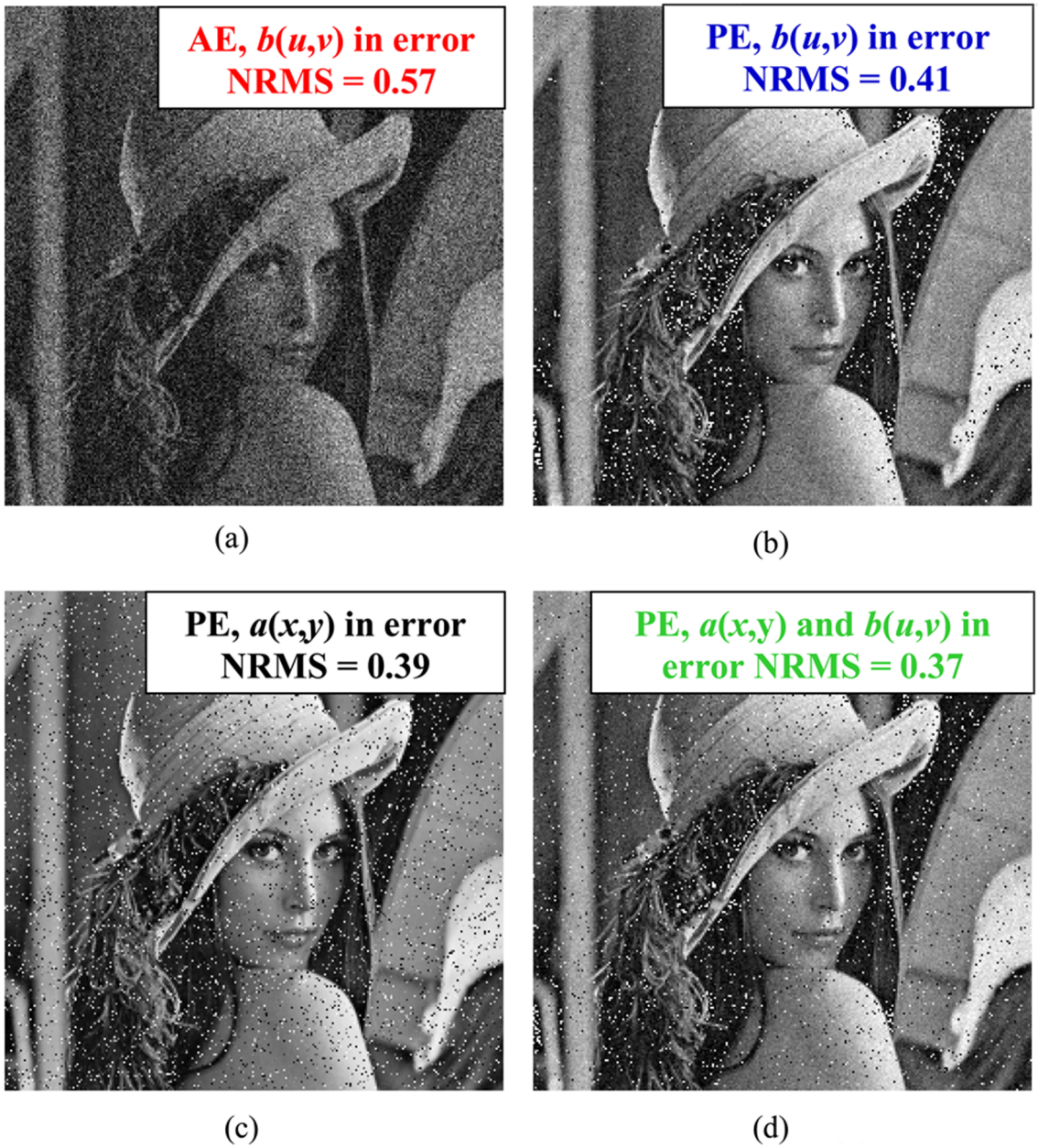

Fig. 7. (Color online) As in Fig. 6 but with 10.07% of the key pixels in error. (a) AE case NRMS of 0.57. (b)–(d) PE case with a NRMS of (a) 0.41, (b) 0.39, and (c) 0.37.

when the graph indicates that 9 bits are beings used in the AE case, 8 of the bits are used in the image-plane key and 1 bit is used in the Fourier-plane key. Comparing the AE and PE cases, it would appear that the AE case is more resilient, having lower error for the same number of bits than the equivalent (circle) PE case.

The results from this simulation suggest that it is advantageous, when attacking, to use an equal number of quantization levels in both the image-plane phase key, $a(x,y)$, and the Fourier-plane phase key, $b(u,v)$. It also suggests that lower-quality spatial light modulators, i.e., spatial light modulators with fewer available phase-quantization levels, may still be applied to produce decrypted images with low levels of NRMS error.

5. Conclusions

In this paper we have performed a numerical analysis of the double random phase encoding (DRPE) technique to determine how, in the amplitude encoding (AE) and phase encoding (PE) cases, the two encryption keys, the image-plane key $a(x,y)$ and Fourier-plane key, $b(u,v)$, used during decryption affect the output image when they have increasing amounts of error. In all cases we have assume an error-free encryption process, and then we have introduced errors into the decrypting phase keys.

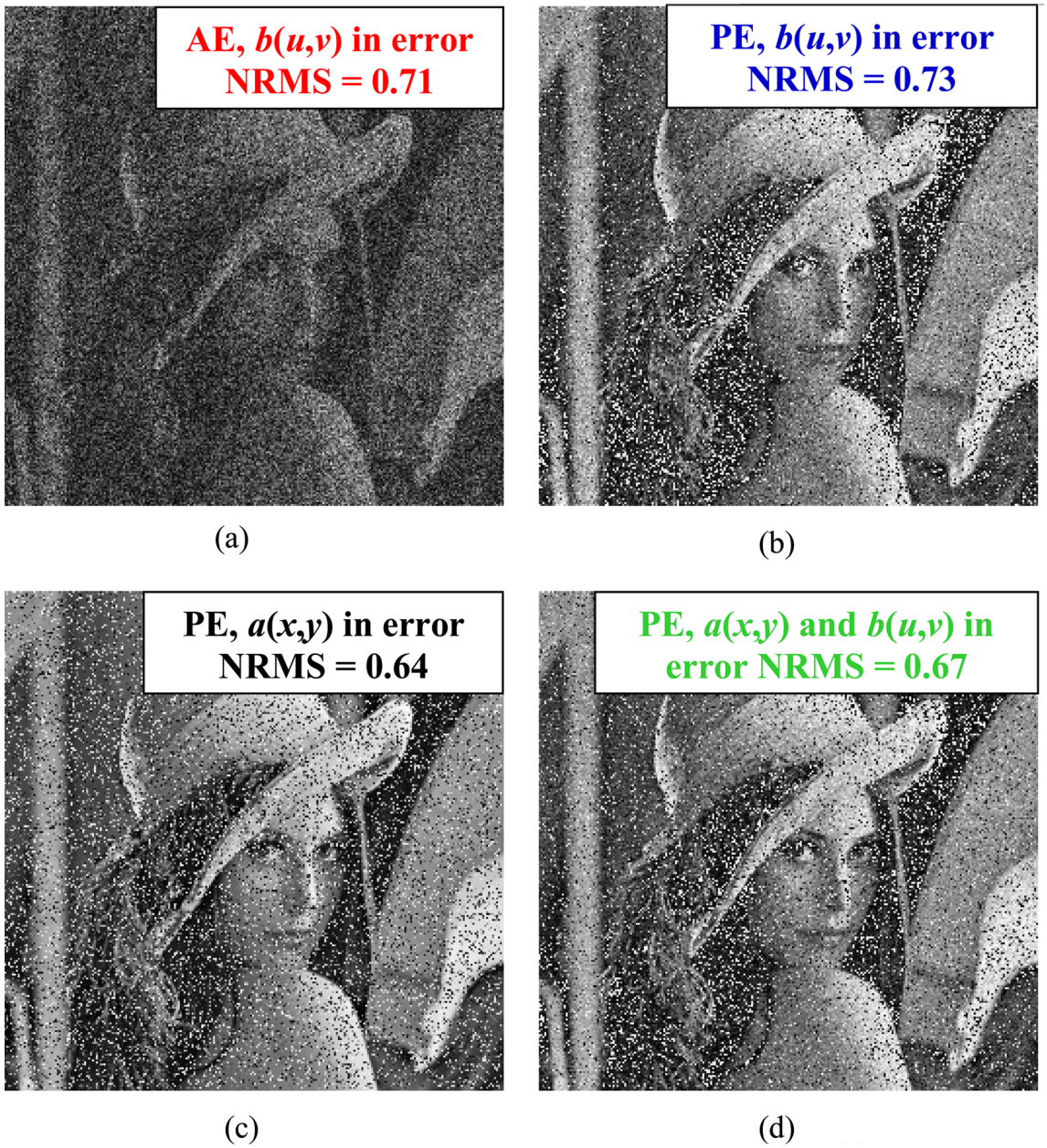

Fig. 8. (Color online) As in Fig. 6 and 7 but with 30.52% of the key pixels in error. (a) AE case NRMS of 0.71. (b)–(d) PE case with a NRMS of (a) 0.73, (b) 0.64, and (c) 0.67.

In this study the PE method proved to be less sensitive to incorrect pixel values in the phase keys than the AE method. However, it should be noted that in the PE case it is necessary to know both of the encrypting phase keys in order to carry out the decryption process, and this significantly increases the complexity of this encoding technique. The simulation results presented suggest that the decryption process is more sensitive to incorrect pixel values in the Fourier-plane phase key than to an equivalent number of pixel errors in the image-plane phase key. Furthermore, it is observed that the resultant noise in the output, decrypted images, produced due to incorrect pixel values in the two phase keys, have different properties. It is noted that errors in the image-plane key, being in the same plane as the output plane, tend to produce salt and pepper noise, while errors in the Fourier-plane result in Gaussian type noise. When the number of quantization levels that can be used in the phase keys during decryption is restricted, for example, because of hardware, storage, or speed requirements, we have shown that using two phase keys of similar size, rather than having one very good quality and one of poorer quality, results in lower errors. We have also found the AE to be less sensitive to errors, and thus easier to break, than the equivalent PE case.

Finally we note that the results presented in this paper were reproduced for several different gray-

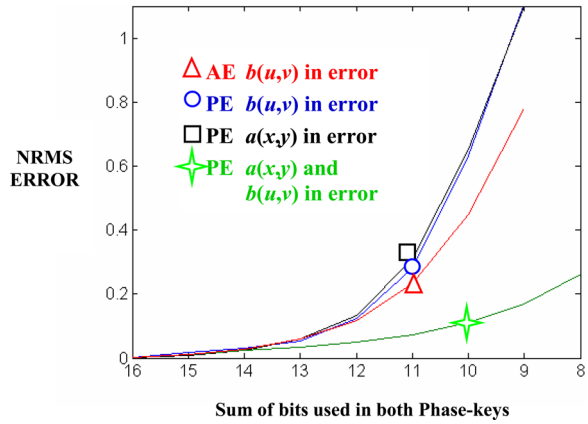

Fig. 9. (Color online) The AE case and the three PE cases where the decrypting phase-keys are requantized at increasingly lower levels, plotted against the resultant NRMS error.

scale input test images. In some of these images the slopes of the results curves varied, but the general trends remained consistent throughout.

We acknowledge the support of Enterprise Ireland and Science Foundation Ireland through the Research Innovation and Proof of Concept Funds, and the Basic Research and Research Frontiers Programmes. We would also like to thank the Irish Research Council for Science, Engineering and Technology. D. S. Monaghan acknowledges the support of the International Society for Optical Engineering (SPIE) through an SPIE Educational Scholarship.

References

1. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
2. B. Javidi, A. Sergent, G. S. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng. **36**, 992–998 (1997).
3. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887–889 (2000).
4. B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, "Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption," Appl. Opt. **39**, 4117–4130 (2000).
5. B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," Optik (Jena) **114**, 251–265 (2003).
6. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," Opt. Express **14**, 3181–3186 (2006).
7. B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," Opt. Eng. **43**, 2239–2249 (2004).
8. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595–6601 (2000).
9. J. W. Goodman and R. W. Lawrence, "Digital image formation from electronically detected holograms," Appl. Phys. Lett. **11**, 77–79 (1967).
10. U. Schnars and W. Juptner, "Direct recording of holograms by a CCD target and numerical reconstruction," Appl. Opt. **33**, 179–181 (1994).
11. G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," Appl. Opt. **46**, 5257–5262 (2007).
12. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253–10265 (2007).
13. "Lena test image," http://sipi.usc.edu/database/.
14. Matlab 7.0.1, http://www.mathworks.com/.
15. G. Unnikrishnan, M. Pohit, and K. Singh, "A polarization encoded optical encryption system using ferroelectric spatial light modulator," Opt. Commun. **185**, 25–31 (2000).
16. U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Polarization encoding and multiplexing of two-dimensional signals: application to image encryption," Appl. Opt. **45**, 5693–5700 (2006).
17. F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," J. Opt. Soc. Am. A **15**, 2629–2638 (1998).
18. W. K. Pratt, *Digital Image Processing*, 4th ed. (Wiley-Interscience, 2007).