Cryptanalysis of optical security systems with significant output images

Guohai Situ, Unnikrishnan Gopinathan, David S. Monaghan, and John T. Sheridan*

School of Electrical, Electronic, and Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland

*Corresponding author: john.sheridan@ucd.ie

Received 2 January 2007; accepted 14 April 2007;
posted 23 April 2007 (Doc. ID 78534); published 9 July 2007

The security of the encryption and verification techniques with significant output images is examined by a known-plaintext attack. We introduce an iterative phase-retrieval algorithm based on multiple intensity measurements to heuristically estimate the phase key in the Fourier domain by several plaintext-cyphertext pairs. We obtain correlation output images with very low error by correlating the estimated key with corresponding random phase masks. Our studies show that the convergence behavior of this algorithm sensitively depends on the starting point. We also demonstrate that this algorithm can be used to attack the double random phase encoding technique. © 2007 Optical Society of America

OCIS codes: 070.2580, 070.4560, 100.5070, 200.4560.

1. Introduction

Optical information security has received much attention over the past decade [1–28]. Various algorithms have been proposed for data encryption [1–10], information hiding [11–14], watermarking [15,16], and verification [17–23]. These algorithms can be implemented optically by taking advantage of both the natural two-dimensional imaging capabilities of optics and the parallelism achievable with optical processing. Although there are some reports in the literature that optical security algorithms are robust against blind decryption [2], these are insufficient to evaluate the strength of such encryption systems. It was not until recently that systematic investigations of strength have been carried out. So far these have mainly focused on the classic double random phase encoding (DRPE) scheme first proposed in 1995. Studies have shown that the DRPE is vulnerable to known-plaintext, chosen-plaintext, and chosen-cyphertext attacks [25–28]. The phase key can be obtained if the attacker has sufficient freedom to use the entire complex cyphertext and the corresponding plaintext, or choose some specific cyphertext [25,26]. Heuristic attack is also possible to find key distributions capable of recovering the plaintext though the result can contain significant amounts of noise [27,28].

We examine the security of other kinds of optical verification systems—those with significant output images. These methods were first proposed by Wang *et al.* [3] in 1996. They employed a modified projection-onto-constraint-sets (POCS) algorithm to encode a plaintext $c(x, y)$ into a random phase distribution $\exp[j\psi(u, v)]$ at the Fourier plane in a 4-f setup relating to a fixed phase mask $\exp[j\phi(x, y)]$. This fixed phase mask acts as the key to the system. When $\exp[j\psi(u, v)]$ is modulated by the spatial frequency spectrum of $\exp[j\phi(x, y)]$, its Fourier transform then produces the significant image $c(x, y)$ at the output. The encoding or encryption process is purely digital, while the decoding can be done either digitally or optically. Later in 2000, Li *et al.* [17] proposed to encode the plaintext $c(x, y)$ into a random phase distribution $\exp[j\phi(x, y)]$ in the spatial domain, rather than in the frequency domain. This results in better decoding quality [24] and makes implementation more convenient. Furthermore, both data encryption and authentication verification can be performed. In all such systems, only the intensities can be measured at the output. Consequently, as stated in Ref. 17, an attacker generally cannot calculate the phase key $\exp[j\psi(u, v)]$, given knowledge of the other phase mask, even if this is available together with the intensity pattern of the corresponding output. This

0003-6935/07/225257-06$15.00/0

property also results in other improvements in security: using some specific inputs such as a delta function it is not possible to obtain the information of $\exp[j\psi(u, v)]$, making it extremely infeasible to find the exact solution with the techniques proposed in Refs. 25 and 26. Therefore it is impossible for an attacker to find the key given knowledge of one phase input R_1 and the corresponding output intensity because of the theory of phase retrieval. However, what if information about more than one such pair is available? Essentially, the output image is the correlation of $\exp[j\phi(x, y)]$ and $\exp[j\psi(u, v)]$ rather than the exact plaintext $c(x, y)$. Even its magnitude must contain information about the key $\exp[j\psi(u, v)]$. Therefore, measuring the intensities of the output patterns corresponding to several inputs may provide sufficient knowledge to crack the key.

In Section 2 we first review the basic principle of the Li *et al.* method [17]. In Section 3 we examine the security of their scheme. In particular, we present an algorithm to extract the key based on multiple measurements of the output intensities, numerically validate the algorithm, and discuss the performance. In Section 4 we show that the algorithm can also be used to crack the classic DRPE system.

2. Basic Principle of the Li *et al.* Security Scheme

The Li *et al.* algorithm [17] is a generalization of the POCS algorithm. Before going through their method, we briefly review the original.

A. POCS Algorithm

Although the POCS algorithm was invented in the early 1980's for the purpose of image restoration [29,30], its basis can be traced further back to 1972, when Gerchberg and Saxton (GS) proposed their algorithm [31]. This algorithm has been widely used in various fields including astronomy, crystallography [32], image restoration, and diffractive optical elements design [33]. These problems generally involve phase retrieval in two domains: For example, given $|G(x_1, y_1)|$, the intensity of the Fourier (or Fresnel) spectrum of an object $g(x_0, y_0)$, find the phase component $\exp[j\beta(x_1, y_1)]$ of the spectrum in order to recover the whole original object:

$$\begin{aligned} g(x_0, y_0) &= |g(x_0, y_0)|\exp[j\alpha(x_0, y_0)] \\ &= \mathcal{P}^{-1}\{|G(x_1, y_1)|\exp[j\beta(x_1, y_1)]\}, \end{aligned} \quad (1)$$

where $\mathcal{P}^{-1}$ represents a transform operator.

This problem becomes easier to solve if we have some additional *a priori* knowledge regarding the magnitude of the object. The POCS algorithm can be described as follows:

Step 1. Initialize the phase component of the frequency spectrum, i.e., choose a starting point for the search.

Step 2. Transform the spectrum consisting of the measured magnitude and the generated phase component to the spatial domain.

Step 3. Impose the object magnitude constraint on the resulting complex amplitude, while retaining its phase unchanged.

Step 4. Transform the modified signal backward to the spectrum domain.

Step 5. Replace the magnitude of spectrum with the original measured data, while retaining the phase unchanged, and return to Step 2.

This iteration process is carried out until a feasible solution of Eq. (1) is found.

B. Li *et al.* Method

The encoding method proposed in Ref. 17 can be regarded as involving a phase retrieval problem in a 4-f system with the knowledge of the phase distribution $\exp[j\psi(u, v)]$ at the Fourier plane and the magnitudes at both the input and the output planes. That is, find a phase distribution, $\exp[j\phi(x, y)]$, that makes the following equation valid:

$$|c(x, y)| = |\mathcal{F}^{-1}\{\mathcal{F}\{\exp[j\phi(x, y)]\}\exp[j\psi(u, v)]\}|, \quad (2)$$

where $\mathcal{F}$ and $\mathcal{F}^{-1}$ represent Fourier and inverse Fourier transforms, respectively. The expected output $|c(x, y)|$ in this equation stands for the correlation image. If, and only if, $|c(x, y)|$ appears on the camera at the output plane as a result of a correlation between the phase key $\exp[j\psi(u, v)]$ and the phase mask $\exp[j\phi(x, y)]$ assigned to a legal user, is the true input verified. On the other hand, as in the Wang *et al.* scheme [3], this can also be used as an encryption method, in which $|c(x, y)|$ is the plaintext and $\exp[j\psi(u, v)]$ acts as the cyphertext.

Although Eq. (2) appears more complex than Eq. (1), it still just involves phase retrieval between two domains, i.e., the input and output. Therefore, this integral equation can be solved with an iteration process similar to that used in the POCS algorithm:

Step 1. Randomly generate a starting value for $\exp[j\phi(x, y)]$.

Step 2. Transform $\exp[j\phi(x, y)]$ to the output plane using Eq. (2), resulting in a complex amplitude $\hat{c}(x, y) = |\hat{c}(x, y)|\exp[j\varphi(x, y)]$.

Step 3. Replace $|\hat{c}(x, y)|$ with $|c(x, y)|$, and transform $|c(x, y)|\exp[j\varphi(x, y)]$ back to the input plane, i.e., $\mathcal{F}^{-1}\{\mathcal{F}\{|c(x, y)|\exp[j\varphi(x, y)]\}\exp[j\psi(u, v)]\}$.

Step 4. Discard the magnitude of the resulting complex amplitude, and update $\exp[j\phi(x, y)]$ with its phase component. Return to Step 2.

In the original proposal [17], the Li *et al.* method involved a preoptimization process of the phase at the Fourier plane $\exp[j\psi(u, v)]$, the purpose of which was to constrain most of the energy of the correlation signal within a predefined area at the camera plane. However, this process does not play an important role in the security of the system. In a more recent paper, in which this algorithm is used for image hiding [11], it is simply represented using a random phase distribution.

3. Cryptanalysis

Cracking the system involves finding the value of the phase $\exp[j\psi(u, v)]$ with some knowledge about the input and the corresponding output of the correlator. However, it is in general not possible to solve Eq. (2) given $\exp[j\phi(x, y)]$ and $|c(x, y)|$ because of the absence of the phase component of the correlation output. The POCS technique, as described in Subsection 2.A may be directly employed to find a feasible phase distribution $\exp[j\psi'(u, v)]$ that, correlating with $\exp[j\phi(x, y)]$, will result in a distinguishable $|c'(x, y)|$ close to $|c(x, y)|$. This $\exp[j\psi'(u, v)]$ is generally quite different from the true key $\exp[j\psi(u, v)]$ because of the multiple-solution nature of the equation. However, using one single $\exp[j\psi(u, v)]$ to produce several phase masks inevitably introduces a risk to security because this "leaks" more information about the key, though in a very indirect manner. In this case, cracking the system comes down to solving the following set of equations:

$$|c_k(x, y)| = \left|\mathcal{F}^{-1}\{\mathcal{F}\{\exp[j\phi_k(x, y)]\}\exp[j\psi(u, v)]\}\right|,$$
$$k = 1, 2, \ldots, K. \tag{3}$$

Even if in the worst case the attackers are unable to gather so many legal input–output pairs, they may use arbitrary phase distribution as the input. The resulting correlation signal will then be a noiselike signal rather than a significant image, The measured output intensities (or magnitudes), $|c_k(x, y)|$, will contain information about $\exp[j\psi(u, v)]$. In this case, Eq. (3) is still valid. Based on these observations we now propose a technique to find the key and thus crack this system.

A. Attackers Algorithm

Solving Eq. (3) can be described as follows: Given K random phase distributions ϕ_k and the corresponding measured magnitudes $|c_k|$, where $k = 1, 2, \ldots, K$, find a phase distribution ψ that makes the following optimization problem valid:

$$\min\left\{\sum_{k=1}^{K} \|\mathcal{P}\{\phi_k, \psi\} - |c_k|\|\right\}, \tag{4}$$

where symbol $\mathcal{P}$ represents the cascaded Fourier transforms as described on the right-hand side of Eq. (3), and $\|\cdot\|$ is the norm. This problem can be solved with a modified POCS algorithm as shown in Fig. 1. It starts with the random generation of the initial phase key as $\psi_1^{(1)}$ and then computes the Fourier transform of the input phase functions $\exp[j\phi_k(x, y)]$:

$$s_k(u, v) = |s_k(u, v)|\exp[j\beta_k(u, v)] = \mathcal{F}\{\exp[j\phi_k(x, y)]\},$$
$$k = 1, 2, \ldots, K. \tag{5}$$

It is easily seen from Fig. 1 that the algorithm mainly consists of two loops: the inner sequentially imposes all the K constraints, while the outer controls the iteration of the inner loop as a whole. For the sake of brevity, we now introduce the following notation. We denote the phase to be evaluated at the nth iteration as $\psi_{k+1}^{(n)}$ given the input–output pairs $\{\phi_k, |c_k|\}$ and the phase $\psi_k^{(n)}$ estimated as a result of the last inner loop. Given $\psi_k^{(n)}$ and ϕ_k, it is easy to compute their correlation:

$$\hat{c}_k^{(n)}(x, y) = \left|\hat{c}_k^{(n)}(x, y)\right|\exp\left[j\varphi_k^{(n)}(x, y)\right] = \mathcal{F}^{-1}\left\{s_k(u, v)\exp\left[j\psi_k^{(n)}(u, v)\right]\right\}. \tag{6}$$

The magnitude $|\hat{c}_k^{(n)}|$ of the resulting correlation is constrained by the *a priori* data $|c_k|$ and the modulated correlation is Fourier transformed backward to the frequency plane

$$\hat{s}_k^{(n)}(u, v) = \left|\hat{s}_k^{(n)}(u, v)\right|\exp\left[j\hat{\beta}_k^{(n)}(u, v)\right] = \mathcal{F}\left\{|c_k(x, y)|\exp\left[j\varphi_k^{(n)}(x, y)\right]\right\}, \tag{7}$$

resulting in the new phase

$$\psi_{k+1}^{(n)} = \hat{\beta}_k^{(n)} - \beta_k. \tag{8}$$

This phase $\psi_{k+1}^{(n)}$ is then used to evaluate the next phase $\psi_{k+2}^{(n)}$, which is then used together with the next pair of measured data $\{\phi_{k+1}, |c_{k+1}|\}$, according to the process described above. This process is repeated until all K pairs of measured data are used for the phase evaluation. When $k = K$, the resulting phase $\psi_{K+1}^{(n)}$ is used as the starting phase for the next iteration

$$\psi_1^{(n+1)} = \psi_{K+1}^{(n)}. \tag{9}$$

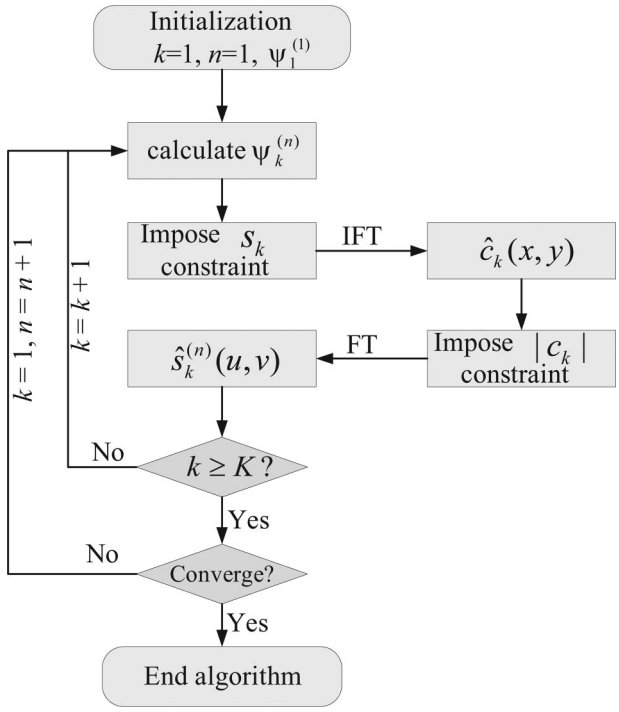
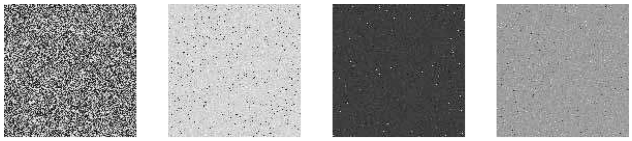
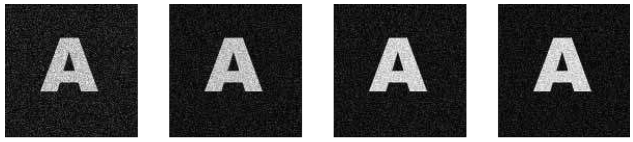


Fig. 1. Flow chart of the attacker algorithm.



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

Fig. 2. Original phase key (a) and the difference between the estimated and original 256-phase levels given (b) 4, (c) 8, and (d) 16 arbitrary input–output pairs.



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

Fig. 4. Decoded images with (a) $K = 4$, (b) $K = 4$, (c) $K = 16$, and (d) Li and Rosen's algorithm [17].

If it converges after N iterations, the optimized distribution for ψ can be written as

$$\hat{\psi} = \psi_{K+1}^{(N)}. \tag{10}$$

B. Validation of the Attack Technique

The attacker's purpose is to find the phase ψ given some known inputs and measurements of the corresponding output intensities. So in computer simulations, we mainly focus on the quality of the recovered phase Eq. (10). Therefore, without any loss of generality, we use random phases, which are uniform distributions between $[0, 2\pi]$, as the inputs. The resulting output magnitudes $|c_k|$ are randomlike noise.

In the first simulation, we assume the distribution of the phase key is nearly continuous. Taking the state-of-the-art manufacturing technology into account, it is reasonable to represent a "continuous" distribution in 256-phase levels. The original phase key is shown in Fig. 2(a), and the differences between the original and these estimated phases are shown in Figs. 2(b)–2(d), respectively. We can see from these figures that the differences are small. This can be shown using histograms of these phase differences in Figs. 3(a)–3(c). It is seen that the histograms for these phase-differences are located at different positions. This reflects that these distributions have different mean values. It is easy to verify that ψ plus any constant distribution is still an exact solution of the equation. It is the standard deviation σ of the phase difference, or intuitively, the width of their histogram, that for all practical purposes influences the decoding performance. In these cases, the σ values are (a) 0.6209, (b) 0.2703, and (c) 0.1537 rad, respectively. This can be more clearly appreciated by examining Figs. 4(a)–4(c), the decoded images with these estimated keys. The decoded image with the original key is shown in Fig. 4(d) for comparison. High-quality outputs were obtained. The normalized mean square errors (NMSE)

$$\mathrm{NMSE} = \frac{\sum_{l=1}^{L}\sum_{m=1}^{M}[\hat{c}(m,\ l) - c(m,\ l)]^2}{\sum_{l=1}^{L}\sum_{m=1}^{M}[c(m,\ l)]^2} \tag{11}$$

between Figs. 4(a)–4(d) and the plaintext are (a) 0.2062, (b) 0.1326, (c) 0.1132, and (d) 0.0963, respectively. This implies that the more information the attacker knows about ψ, the higher the fidelity that is obtainable. If the same ψ was also used to produce many phase masks corresponding to different images, the attacker can use the estimated phase ψ_{opt} to recover all these images. Figure 5 demonstrates several such successful attempts.

The security risk becomes more serious in the case in which a binary key is employed. We have observed that it is in this case very easy to find the key distribution with extremely high fidelity, especially when many $\{\phi,\ |c|\}$ pairs (for example, $K = 16$) are used. Figure 6(a) shows the binary key for the simulation. The differences between it and the estimated phases when $K = 4$, 8, and 16 are shown in Figs. 6(b)–6(d), respectively. The number of incorrect phase pixels is just (b) 537, (c) 135, and (d) 13, resulting in an error rate of (b) 0.0328, (c) 0.0082, and (d) 7.9346×10^{-4}, respectively.

C. Convergence of the Algorithm

The attacker's algorithm presented in Subsection 3.A can be seen as some kind of generalization of the POCS algorithm for multiple intensity measurements. In this sense, the iteration process can be concisely rewritten in the form of

$$\psi^{(n+1)} = \mathcal{P}_1\mathcal{P}_2 \ldots \mathcal{P}_I\psi^{(n)}, \tag{12}$$

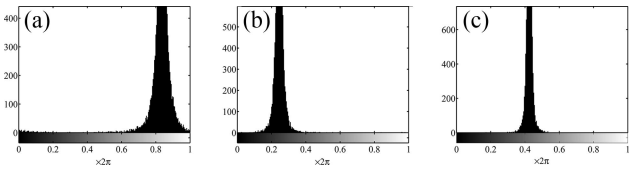
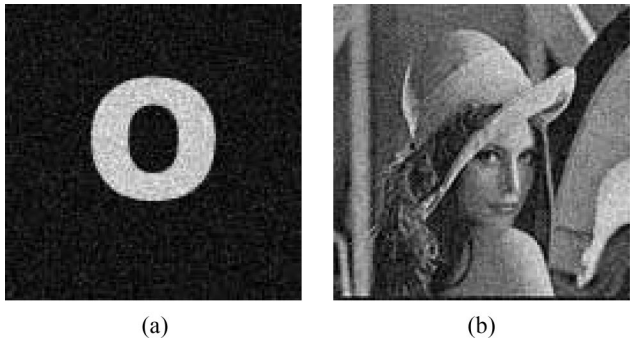
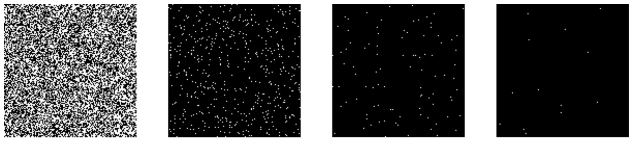


Fig. 3. Histograms of the distributions in Figs. 2(b)–2(d).



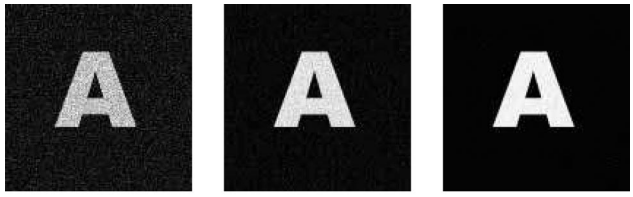
(a) (b)

Fig. 5. Demonstration of using the cracked phase to obtain other correlation significant images previously encoded with the same ψ.



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

Fig. 6. (a) Original binary phase key and the difference between the recovered and the original binary phase keys from (b) 4, (c) 8, and (d) 16 intensity measurements.



(a) (b) (c)

Fig. 8. Decrypted images with the extracted phase key.

where symbols $\mathcal{P}_i$, $i = 1, 2, \ldots, I$, are the projection operators onto a series of constraint sets. Normally, these sets include

$\mathbb{C}^{\mathrm{P}}$: the phase-only constraint for the phase key $R_2 = \exp[j\psi]$, i.e., $\mathbb{C}^{\mathrm{P}} = \{R_2 \in \mathbb{L}^2 : |R_2| = 1\}$;

$\mathbb{C}_k^{\mathrm{M}}$: all the K constraints imposed by the measured magnitudes at the output plane, i.e., $\mathbb{C}_k^{\mathrm{M}} = \{R_2 \in \mathbb{L}^2 : |\mathcal{P}\{\phi_k, R_2\}| = |c_k|\}$ for $k = 1, 2, \ldots, K$;

$\mathbb{C}^{\mathrm{Q}}$: the quantization constraint of the phase if ψ is quantized, $\mathbb{C}^{\mathrm{Q}} = \{\psi \equiv 2q\pi/Q \bmod 2\pi : q, Q \in \mathbb{N}, q \le Q\}$.

These sets are all nonconvex. Note that there are K sets corresponding to the magnitude constraints. The overall number of these nonconvex sets is usually larger than the number of intensity measurements, i.e., $I > K$. According to our experience, at least three $\{\phi, |c|\}$ pairs should be used to obtain a successful attack, i.e., $K \ge 3$. As a consequence, the number of the nonconvex sets is always larger than 2. According to the Levi–Stark theorem [30], the attacker's algorithm therefore does not guarantee convergence theoretically for every trial. Fortunately, however, convergence is always observed in practice with a probability of a little more than 0.5, i.e., an attacker will crack the system successfully in 50% of all attempts starting with an arbitrary $\psi^{(1)}$.

Obviously, as in the case of the normal POCS, the convergence behavior of the cracking algorithm is quite sensitive to the starting point $\psi^{(1)}$. Take, for example, the case of $K = 4$, and ψ involving 256 phase levels. In this case the algorithm converged within 300 iterations for about 30% initialization of $\psi^{(1)}$; however, it may need significantly more iterations for others. In other worst cases of stagnation [30,34], trapping, tunneling, and even divergence have been observed in our simulations. Fortunately, these distinct behaviors can be easily detected by examining the evolution of the error value within 50 iterations. We note that the computation complexity of the algorithm is $2NK \times T \log_2 T$, where $T = ML$ is the total number of sampling points of the phase. It takes no more than 2 min for a modern Pentium D PC with 1 GB memory to judge the convergence characteristics for $K = 16$, and $T = 128 \times 128 = 16{,}384$. In such case it is then convenient to terminate the iteration and select another starting point. The convergence behavior is also influenced by the number of intensity measurements, especially in the case of binary phase. For $K = 4$, typically more than 1000 iterations are required for convergence (if poor convergence is observed, then termination after 2 min and reinitialization takes place as discussed earlier). But for $K = 8$, the number of iterations has been observed to decrease steeply to about 100. Typical behavior of the NMSE value Eq. (11) during the iteration is plotted in Fig. 7.

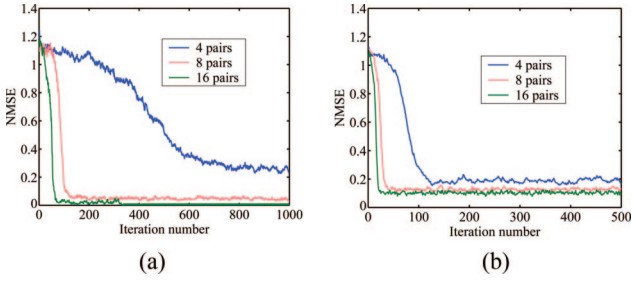


Fig. 7. (Color online) Convergence behavior of the algorithm: phase of (a) binary and (b) 256 gray scale.

4. Cracking the DRPE

The algorithm described above can also be adopted to crack the double random phase encoding systems, especially when the decryption machine is designed in the way that makes some chosen-cyphertext inputs invalid. For instance, if it just allows intensity measurement at the output, choosing a δ function as the cyphertext input cannot directly reveal the information of the phase key at the Fourier plane because in this case the phase component of its Fourier spectrum is unavailable. To apply this algorithm to the DRPE, the attacker needs temporary access to the decryption machine (directly or indirectly) to gather information about the key by measuring several output intensities, which correspond to some predefined input signals, e.g., random phase distributions. It is then relatively easy to find the key following the iteration process described in Subsection 3.A. The decrypted images with (a) 4, (b) 8, and (c) 16 intensity measurements in the case of binary phase are shown in Fig. 8. The values of NMSE for these figures are (a) 0.1311, (b) 0.0269, and (c) 0.0045, respectively.

5. Conclusion

We have examined the security of the Li *et al.* [17] encryption and verification technique with significant output images. We introduced a generalization of the POCS algorithm based on multiple intensity measurements to estimate the phase key ψ in the

Fourier domain. This estimated key $\hat{\psi}$ could correlate with any random phase mask ϕ produced by the same ψ using the Li *et al.* algorithm, resulting in a correlation output with very low error. Our study showed that the convergence behavior of this algorithm sensitively depends on the starting point $\psi_1^{(1)}$. However we have observed that an attacker can crack the system successfully with a probability of 50% of all trials with whatever initialization. We also have demonstrated that this algorithm can be used to attack the DRPE technique as well. This algorithm uses more plaintexts (although they are meaningless random distributions) and magnitudes of the corresponding cyphertexts to evaluate the phase key. It can therefore be classed as a known-plaintext attack, [35] although only the output intensities are known.

Although we just demonstrated the validity of the algorithm for cracking such security systems based on the 4-f setup, it is worth pointing out that a slight modification would be possible to crack those based on similar phase-retrieval techniques in a joint transform correlator [18,19]. Extensions of this algorithm to crack the DRPE systems operating in the fractional Fourier [5] or Fresnel [9] domain are possible.

G. Situ acknowledges the support from the Irish Research Council for Science, Engineering, and Technology. This research is also funded by Science Foundation Ireland and Enterprise Ireland.

References

1. B. Javidi, ed., *Optical and Digital Techniques for Information Security* (Springer Verlag, 2005).
2. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20,** 767–769 (1995).
3. R. K. Wang, L. A. Watson, and C. Chatwin, "Random phase encoding for optical security," Opt. Eng. **35,** 2464–2469 (1996).
4. P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," Opt. Lett. **25,** 566–568 (2000).
5. 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).
6. B. Hennelly and J. T. Sheridan, "Fractional Fourier transform-based image encryption: phase retrieval algorithm," Opt. Commun. **226,** 61–80 (2003).
7. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24,** 762–764 (1999).
8. G. Situ and J. Zhang, "A lensless optical security system based on computer-generated phase only masks," Opt. Commun. **232,** 115–122 (2004).
9. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29,** 1584–1586 (2004).
10. L. Chen and D. Zhao, "Optical image encryption with Hartley transforms," Opt. Lett. **31,** 3438–3440 (2006).
11. J. Rosen and B. Javidi, "Hidden images in halftone pictures," Appl. Opt. **40,** 3346–3353 (2001).
12. J. J. Kim, J. H. Kim, and E. S. Kim, "Optodigital implementation of multiple information hiding and extraction system," Opt. Eng. **43,** 113–125 (2004).
13. Y. Hayasaki, Y. Matsuba, A. Nagaoka, H. Yamamoto, and N. Nishida, "Hiding an image with a light-scattering medium and use of a contrast-discrimination method for readout," Appl. Opt. **43,** 1552–1558 (2004).
14. G. Situ and J. Zhang, "Image hiding with computer-generated phase codes for optical authentication," Opt. Commun. **245,** 55–65 (2005).
15. N. Takai and Y. Mifune, "Digital watermarking by a holographic technique," Appl. Opt. **43,** 3078–3084 (2002).
16. S. Kishk and B. Javidi, "3D object watermarking by a 3D hidden object," Opt. Express **11,** 874–888 (2003).
17. Y. Li, K. Kreske, and J. Rosen, "Security and encryption optical systems based on a correlator with significant output images," Appl. Opt. **39,** 5295–5301 (2000).
18. D. Abookasis, O. Arazi, J. Rosen, and B. Javidi, "Security optical systems based on a joint transform correlator with significant output images," Opt. Eng. **40,** 1584–1589 (2001).
19. M. Yamazaki and J. Ohtsubo, "Optimization of encrypted holograms in optical security systems," Opt. Eng. **40,** 132–137 (2001).
20. D. Abookasis, A. Batikoff, H. Famini, and J. Rosen, "Performance comparison of iterative algorithms for generating digital correlation holograms used in optical security systems," Appl. Opt. **45,** 4617–4624 (2006).
21. H. T. Chang, W. C. Lu, and C. J. Kuo, "Multiple-phase retrieval for optical security systems by use of random-phase encoding," Appl. Opt. **41,** 4815–4834 (2002).
22. G. Situ and J. Zhang, "A cascaded iterative Fourier transform algorithm for optical security applications," Optik **114,** 473–477 (2003).
23. X. F. Meng, L. Z Cai, X. L. Yang, X. X. Shen, and G. Y. Dong, "Information security system by iterative multiple-phase retrieval and pixel random permutation," Appl. Opt. **45,** 3289–3297 (2006).
24. G. Situ and J. Zhang, "Phase-retrieval algorithms applied in a 4-f system for optical image encryption—a comparison," in *Information Optics and Photonics Technology,* G. Mu, F. T. S. Yu, and S. Jutamulia, eds., Proc. SPIE **5642,** 108–115 (2005).
25. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30,** 1644–1646 (2005).
26. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Security analysis of optical encryption," in *Optics and Photonics for Defence and Security,* E. M. Carapezza, ed., Proc. SPIE **5986,** 25–34 (2005).
27. 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).
28. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31,** 1044–1046 (2006).
29. D. C. Youla and H. Webb, "Image restoration by the method of convex projections: part 1—theory," IEEE Trans. Med. Imaging **MI-1,** 81–94 (1982).
30. A. Levi and H. Stark, "Image restoration by the method of generalized projections with application to restoration from magnitude," J. Opt. Soc. Am. A **1,** 932–943 (1984).
31. R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of phase from image and diffraction-plane pictures," Optik **35,** 237–246 (1972).
32. J. R. Fienup, "Phase retrieval algorithms: a comparison," Appl. Opt. **21,** 2758–2769 (1982).
33. H. P. Herzig, "Design of refractive and diffractive micro-optics," in *Micro-Optics,* H. P. Herzig, ed. (Taylor & Francis, 1996), 1–29.
34. H. Stark, Y. Yang, and D. Gurkan, "Factors affecting convergence in the design of diffractive optics by iterative vector-space methods," J. Opt. Soc. Am. A **16,** 149–159 (1999).
35. W. Stallings, *Cryptography and Network Security,* 3rd ed. (Prentice Hall, 2004).