Security and encryption optical systems based on a correlator with significant output images

Youzhi Li, Kathi Kreske, and Joseph Rosen

An improved optical security system based on two phase-only computer-generated masks is proposed. The two transparencies are placed together in a 4*f* correlator so that a known output image is received. In addition to simple verification, our security system is capable of identifying the type of input mask according to the corresponding output image it generates. The two phase masks are designed with an iterative optimization algorithm with constraints in the input and the output domains. A simulation is presented with the resultant images formed by the two phase-only elements. Various mask combinations are compared to show that a combination is unique and cannot be duplicated. This uniqueness is an advantage in security systems. © 2000 Optical Society of America

OCIS codes: 070.4550, 070.2580, 050.1950, 070.6110, 100.5090.

1. Introduction

Optical technologies have recently been employed in data security.[1–4] Compared with traditional computer and electrical systems, optical technologies offer primarily two types of benefits. (1) Optical systems have an inherent capability for parallel processing, that is, rapid transmission of information. (2) Information can be hidden in any of several dimensions, such as phase or spatial frequency; that is, optical systems have excellent capability for encoding information.

In several pioneering studies[1–3] the authors demonstrated different optical verification systems for information security applications, based on optical correlations. These systems correlate two functions: one, the lock, is always inside the correlator, and the other, the key, is presented to the system by the user in the verification stage. Mostly, the systems determine whether the input is true or false by detecting the correlation peak in the output plane. The next generation of these security systems should offer a higher level of security and more sophisticated services than the simple verification offered by the ex-

isting systems. In this paper we propose an optical security system that is based on existing optical correlators but has some additional benefits over those of the present generation.

The first property we intend to improve is the security level of the verification systems. It seems to us that the Achilles' heel of the existing systems is that the output of the optical system is a single narrow intense spot of light, the correlation peak. This peak of light is detected by an intensity detector or a camera and converted to an electronic signal. If the signal is above some predefined threshold, the input mask is verified as the true input. We believe that this procedure has a weakness, because unauthorized intruders may bypass the correlator and illuminate the camera from the outside with a sufficiently intense light spot to cause a false verification. In addition, the complete information of the key mask is given in the lock and vice versa. This is because the key function is equal to the complex conjugate of the Fourier transform of the lock function. That means that the reading of one phase mask by some phase-contrast technique permits a counterfeiting of the other mask. To overcome these drawbacks, we suggest replacing the single spot with a collection of light points ordered in some predefined code or creating an image. This image is confidential and known only to the system designer. If and only if this image appears on the camera plane as a result of a correlation between two masks, the true input is verified. Therefore knowing one phase mask does not permit a person to know the distribution of the other. Even if a person in addition knows the expected image in the
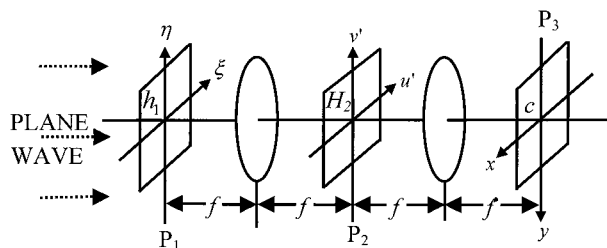
Fig. 1.   4f correlator used for optical security verification.

output, he cannot compute the other mask's values. He also needs to know the phase distribution of the output image to calculate the missing phase mask. However, the phase distribution of the output image can be measured only when the two masks exist inside the system performing the correlation process between their functions.

As we shall see, the same system with the same filter can yield many images for different input masks. This property is an additional benefit of the proposed system. It can verify more than one kind of true input and identify the type of input. Let us compare the existing and the proposed systems with a real example. In a secured plant, for instance, the existing verification systems[1–3] can let someone enter or block that person from entering. Our system can do the same, but in addition it can identify the authorized person that asks to enter and distinguish him from other authorized persons. That is because each person gets a different key function, which yields a different image in the system's output, when the key mask is introduced in the input.

To bypass the correlator illegally is impossible now unless the intruder knows the expected image and can project this image onto the output camera. One can argue that, because the correlator's yield is an image, this image should be automatically recognized. If a second optical correlator is added to recognize the yield of the first one, the output result of the second correlator is a correlation peak, which can be counterfeited in this stage. Our reply to this argument is that optical pattern recognition is not always the best option. If the image is binary with a simple shape or is some code such as a bar code and it appears alone on the output plane at more or less the same location, it can easily be recognized by a digital computer with appropriate software. Breaking into a digital pattern-recognition system seems harder than just illuminating the camera with intense light spot. Although having the verification process in two stages adds complexity, it offers two new benefits: (1) improvement of the security level and (2) more information about the verified user.

To make the concept clearer, let us precisely define the design problem of the proposed system. The system, shown in Fig. 1, is an optical correlator in a 4f configuration with three domains: the input domain in which the input mask h_1 is displayed, the Fourier domain in which the filter mask H_2 is displayed, and the correlation domain in which the camera should

record the output predefined image. h_1 is employed as a kind of a key, whereas H_2 is used as a lock that always exists within the system. The predefined image is built up at the correlation plane P_3 only if the true key h_1 appears in the input. Otherwise, a scattered meaningless light distribution is expected there. Like in the systems of Refs. 1–3, and for the same reasons, both the masks h_1 and H_2 are chosen to be phase-only valued. That is because the phase distribution of phase-only transparencies, compared with the distribution of absorption masks, is hardly deciphered. The output image, obtained on the correlation plane, is constructed from an electromagnetic field projected onto this plane. Thus the image is represented by the complex values of this field. However, the camera can record only the light intensity that is proportional to the square magnitude of the electromagnetic field. Therefore the image's phase distribution actually creates a degree of freedom for the present problem, meaning that it can get any value between 0 to 2π. The problem is to find two phase masks located at two different planes of the correlator, which together should yield on the output plane some function whose magnitude is equal to a predefined image. In other words, the problem is actually an optimization under constraints, in which one needs to find two transparency functions that yield the result closest to the desired image. In this study we solve the optimization problem by a procedure similar to that suggested in Ref. 5. This procedure is a generalization of the algorithm known by the name projection-onto-constraint sets (POCS) (sometimes "constraint" is replaced by "convex"[6]). Basically, in the POCS algorithm a function is transformed back and forth between two domains. At each domain the appropriate constraints are placed until the function converges, in the sense that the final error between the desired and the obtained images is minimal. Wang et al.[4] have proposed an algorithm similar to the POCS, called the phase-retrieval algorithm, for security applications. However, their algorithm produces the phase mask at the spatial-frequency plane (designated here as H_2) and not the input phase mask h_1, as in our case. Therefore their algorithm is good only for producing a single pair of phase masks, one for the input plane and the other for the spatial-frequency plane. Creating many masks at the spatial-frequency plane for the same single input mask is useless, because alignment problems do not permit use of the spatial-frequency plane as the input of the system. However, our algorithm can produce any desired number of input phase masks (many keys) for the same single phase-only filter (single lock) at the spatial-frequency plane. As a result, our method offers the additional service of identifying the type of input mask according to the corresponding output image it generates. The various output codes used to design the many input masks can give, in addition to simple verification, relevant information on the verified user or product. For example, if the input phase mask is part of a bill of paper money, as sug-

gested in Ref. 1, we can design a verification system of bills that yields a series of codes, each of which would contain information on, for instance, the printing date and location of every bill. To the best of our knowledge, this additional service of coding information in the key function was not proposed in Ref. 4 or in other studies.

The algorithm is explained in detail in Section 2, but before that we note that an additional application can be realized by the proposed system. The same setup and the same algorithm are suitable for encryption as well. Let us consider the image in the correlation plane P_3 as the information that we wish to encrypt. The same optimization algorithm yields two phase functions, h_1 and H_2. One of them, say h_1, is the encrypted data, whereas the other function, H_2, is employed as the decipher of this encrypted data. Placing h_1 in the input plane of the correlator, in which H_2 is positioned in its Fourier plane, is the only way to reconstruct the original image. In comparison with other optical encryption systems,[7,8] the encryption process in our system is iterative and digital. The deciphering can be done either digitally or optically. However, the main advantage of this method comes from the nature of the encrypted data. Unlike in other methods,[7,8] the encrypted data appear now as a phase-only function. This means that the amount of data in the encrypted function is half the general complex function with the same size; such phase functions are difficult to read with conventional detection devices.

2. Analysis

With regard to the 4f correlator shown in Fig. 1, the information is encoded into two phase-only computer-generated masks. One is located in the input plane, denoted by $h_1(\xi, \eta) = \exp[j\phi(\xi, \eta)]$, and the other is in the spatial-frequency plane, denoted by $H_2(u, v) = \exp[j\Phi(u, v)]$. In this system the output at the correlation plane is given by

$$c(x, y) = \Im^{-1}\{\Im\{h_1(\xi, \eta)\}H_2(u, v)\}$$
$$= \Im^{-1}\{\Im\{h_1(\xi, \eta)\}\exp[j\Phi(u, v)]\}, \quad (1)$$

where $\Im$ and $\Im^{-1}$ denote the Fourier transform (FT) and the inverse FT, respectively. For notation simplicity we assume that (u, v) are the spatial-frequency variables related to the spatial coordinates (u', v') by the relation $(u, v) = (u', v')/\lambda f$. The expected system's output is

$$c(x, y) = A(x, y)\exp[j\psi(x, y)], \quad (2)$$

where $A(x, y)$ is the amplitude of the expected output image and $\psi(x, y)$ denotes the phase of $c(x, y)$. From Eq. (1) the input function is given by

$$h_1(\xi, \eta) = \Im^{-1}\left\{\frac{\Im\{c(x, y)\}}{H_2(u, v)}\right\}$$
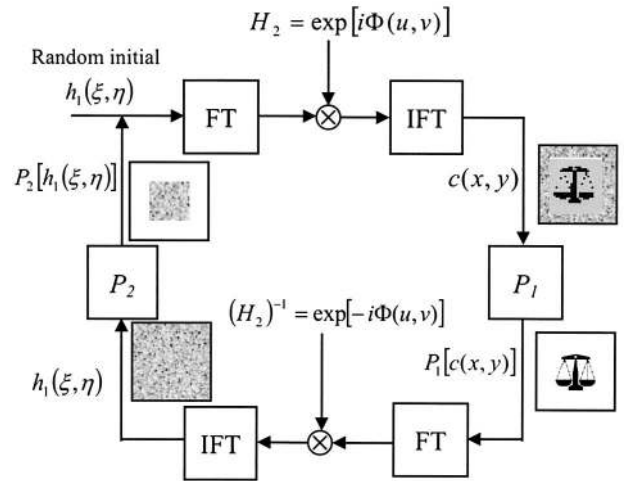$$= \Im^{-1}\{\Im\{c(x, y)\}\exp[-j\Phi(u, v)]\}. \quad (3)$$

Fig. 2. Block diagram of the main POCS algorithm used to compute the phase-only mask $h_1(\xi, \eta)$.

To design two phase-only masks that produce an output image with a given magnitude, we choose to use the generalized POCS algorithm. This iterative algorithm starts with a random function for the first $h_1(\xi, \eta)$. Then the function $h_1(\xi, \eta)$ is transformed by the correlation, defined in Eq. (1), into the output function $c(x, y)$ and then back through the inverse correlation defined by Eq. (3). At every iteration, in each of the two domains (x, y) and (ξ, η), the obtained functions are projected onto the constraint sets. In the (x, y) domain the constraint set expresses the expectations to get the predefined image. In the (ξ, η) domain the constraint set manifests the limitation on the input function to be a phase-only function. The algorithm continues to circulate between the two domains until the error between the actual and the desired output functions is no longer meaningfully reduced.

As mentioned above, the constraint in the output plane should reflect the desire to get the image expressed by the positive function $A(x, y)$. Therefore in the output plane the projection P_1 on the constraint set is

$$P_1[c(x, y)] = A(x, y)\exp[j\psi(x, y)], \quad (4)$$

where $A(x, y)$ is a real positive function representing the output image. In the input plane we recall that $h_1(\xi, \eta)$ should be a phase-only function, and therefore the projection P_2 on the constraint set is

$$P_2[h_1(\xi, \eta)] = \begin{cases} \exp[j\phi(\xi, \eta)] & \text{if } (\xi, \eta) \in W \\ 0 & \text{otherwise} \end{cases}, \quad (5)$$

where $\phi(x, y)$ denotes the phase of $h_1(\xi, \eta)$, that is, $\exp[j\phi(\xi, \eta)] = h_1(\xi, \eta)/|h_1(\xi, \eta)|$, and W is a window function that is necessary for reasons described in Section 3. The iteration process is shown schematically in Fig. 2. Note that $H_2(u, v)$ is chosen only once before the beginning of the iterations, in a process that will be explained below. After $H_2(u, v)$ is

(a)

(b)

Fig. 3. Two expected output images of the correlator used in the computer simulation.

Fig. 5. Phase function of the mask $H_2(u, v)$.

defined, it becomes part of the correlator and is never changed during the circulating process.

The convergence of the algorithm to the desired image in the nth iteration is evaluated by the average mean-square error e_n between the intensity of the correlation function before and after the projection, as follows,

$$e_n = \frac{1}{M} \int\int \left|\, \left|\, P_1[c(x, y)]\right|^2 - \gamma_n |c_n(x, y)|^2 \right|^2 \, \mathrm{d}x\mathrm{d}y, \quad (6)$$

where γ_n is a matching constant[9] determined to minimize e_n and M is the total area of the output plane. When the reduction rate of this error function becomes slower than some predefined value, the iterations are stopped.

As discussed in Ref. 5, there are two conditions that guarantee that this error will never diverge. First, the correlator should be an energy-conserving

operator. This property is easily achieved if $H_2(u, v)$ is a phase-only function, as indeed it is in the present case. The second condition to satisfy the nondiverging feature is realized if, among all the functions that belong to the constraint sets, the two projected functions in the nth iteration, $P_1[c_n(x, y)]$ and $P_2[h_{1,n}(\xi, \eta)]$ are the functions closest (by mean of the mean-square metric) to the functions $c_n(x, y)$ and $h_{1,n}(\xi, \eta)$, respectively. It is easy to show that the second condition is also fulfilled in the present algorithm. Therefore the POCS algorithm here can never diverge. Note that the nondiverging feature of the algorithm is an additional reason to

Fig. 4. Block diagram of the mini POCS algorithm used to compute the phase-only mask $H_2(u, v)$.
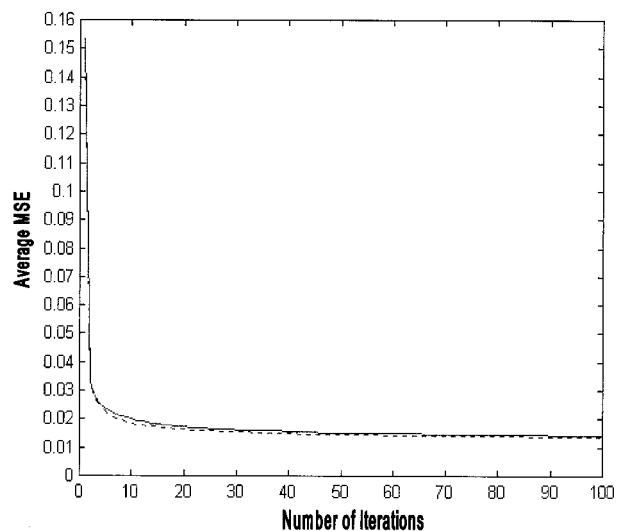
Fig. 6. Average mean-square error (MSE) versus the iterations number for the POCS algorithm in the case of the scale (solid curve) and the duck (dashed curve).
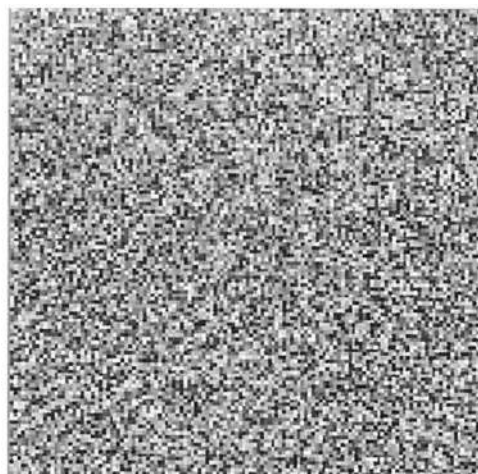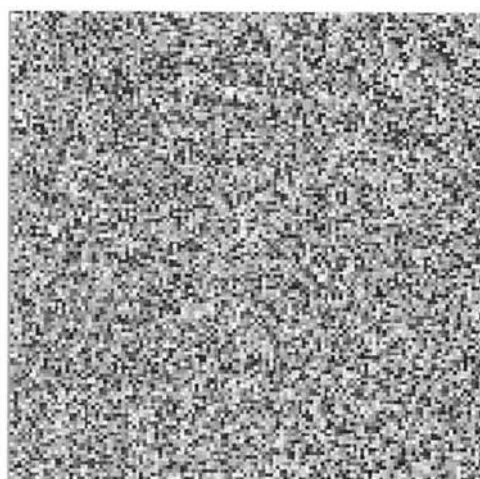
Fig. 7. Phase distributions of $h_1(\xi, \eta)$ for the output images of (a) the duck and (b) the scale.

favor phase-only functions in the spatial-frequency domain.

3. Simulation Results

We wrote a computer simulation demonstrating our general concept discussed above. In our simulations the algorithm was tested with two different binary images as shown in Fig. 3; one (a) is a duck smashing a computer, and the other (b) is a scale. The images comprise 120×120 pixels, whereas the input and the output planes have 256×256 pixels each. In the input domain the two correlated functions are made to cover only the central area of 128×128 pixels, designated as the window W. All the rest of the matrix outside this window is padded with zeros. This ensures that the computer simulation based on discrete FT truly simulates the analog optical system. The signal transformed by the discrete FT is considered periodical. Therefore correlation between two functions that are extended beyond the central window W causes corre-
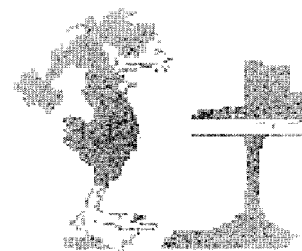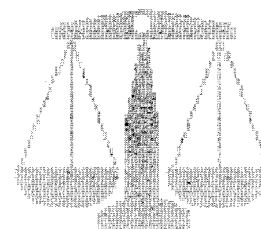
Fig. 8. Resultant images of $|c(x, y)|^2$ for (a) the duck and (b) the scale.

lation between different cycles of the signals, a phenomenon that does not exist in the optical correlator. Padding the input plane with zeros outside the window is done on $h_1(\xi, \eta)$ at every iteration by the projection P_2, defined in Eq. (5). To generate $H_2(u, v)$ so that in the input domain $h_2(\xi, \eta)$ will also cover only the window area, a mini POCS algorithm was introduced. This algorithm generates $H_2(u, v)$ with phase-only values, whereas its inverse FT $h_2(\xi, \eta)$ can get any complex value inside the window W and zero outside it. This mini POCS algorithm is shown schematically in Fig. 4. In this mini POCS algorithm the projection onto the constraint set in the Fourier domain is

$$P_1'[H_2(u, v)] = \exp[j\Phi(u, v)], \qquad (7)$$

where, as defined above, $\exp[i\Phi(u, v)]$ is the phase of function $H_2(u, v)$. In the input domain the projection on $h_2(\xi, \eta)$ is

$$P_2'[h_2(\xi, \eta)] = \begin{cases} h_2(\xi, \eta) & \text{if } (\xi, \eta) \in W, \\ 0 & \text{otherwise} \end{cases}, \qquad (8)$$

where W is the window defined above.

This time the average mean-square error function in the nth iteration is defined as

$$e_n' = \frac{1}{B} \iint_B |h_{2,n}(\xi, \eta)|^2 d\xi d\eta, \qquad (9)$$

where B is the area surrounding the window W (i.e., $B \cup W = M$). In this simulation the average error is less than 0.1% of the maximum value of $h_2(\xi, \eta)$ after

only 30 iterations. Figure 5 shows the phase of $H_2(u, v)$ obtained with 30 iterations of the mini POCS.

$H_2(u, v)$ was calculated only once by the mini POCS and then introduced into the correlator at the spatial-frequency plane. With the same $H_2(u, v)$, we calculated two different input functions $h_1(\xi, \eta)$, for the two images, using the main POCS algorithm described in Section 2. Note that, because the function $H_2(u, v)$ is a random-valued function, there is no limitation by H_2 on the number of different output patterns that can be created by the same single H_2 and many different h_1 functions. The only limitation is the number of patterns that can be drawn on a finite-sized matrix. For both images the algorithm was terminated after 100 iterations. The error plots for both experiments are shown in Fig. 6. The final average errors are less than 2% of the average value of the image, for both images. Figures 7(a) and 7(b) show the phase functions of the two masks h_1 for the expected output images shown in Figs. 3(a) and 3(b),

respectively. We examined the randomness of the resulted masks in comparison with the random masks with which the iterative process starts. It appears that the randomness is the same even after 100 iterations. The phase values are still distributed uniformly, and the autocorrelation width is still one pixel, which indicates that the phase values are mutually independent.

The resultant correlation functions $|c(x, y)|^2$ after 100 iterations can be seen in Fig. 8. The camera records the noisy images shown in Fig. 8, and the value of each pixel is compared with a predefined threshold. To examine the efficiency of the algorithm and the immunity of the resulted images from noise, we define a test measure termed error–immunity ratio (EIR), as follows:

$$EIR = \frac{(\text{minimum value of the image intensity}) - (\text{maximum value of the background intensity})}{(\text{minimum value of the image intensity}) + (\text{maximum value of the background intensity})}.$$

The EIR is a quantity between 0 and 1, which indicates the immunity of the threshold procedure from making erroneous decisions. For the images shown in Fig. 8 the EIR's are 0.63 and 0.66, respectively.

The final question we consider here is whether the

Fig. 9. Table of all cross correlations between functions h_1 and the inverse FT of functions H_2. The second index of each function denotes the number of the process used to design the functions. Only the pairs that were designed together at the same process yield the image of the scale.

two phase functions $h_1(\xi, \eta)$ and $H_2(u, v)$ can be deciphered when we know the image function $A(x, y)$. Because each process of POCS starts with a random function as the first trial, the final solutions are always different from one experiment to another, although all of them yield the same desired image on the correlation plane. Therefore even if some unauthorized intruder acquires the predefined image in the output plane, he would not be able to reproduce the masks $H_2(u, v)$ and $h_1(\xi, \eta)$ to get access to the system. This feature is demonstrated in the table shown in Fig. 9. Five pairs of $H_2(u, v)$ and $h_1(\xi, \eta)$ were calculated for the same image of the scale by the mini and the main POCS. This table shows the correlation intensity between any possible pair $h_{1,i}(\xi, \eta)$ and $\Im^{-1}\{H_{2,j}(u, v)\}$. Only the pairs, calculated together in the same process, yield the desired image, as seen along the diagonal of the table. All the rest of the cross correlations yield scattered meaningless distributions. The conclusion is that, even if the image is known, it is impossible to deduce the right $h_1(\xi, \eta)$ for an unknown $H_2(u, v)$.

4. Conclusions

We have developed a method to design an optical security system based on computer-generated optical diffractive elements. According to our method, one can design two phase-only transparencies for a $4f$ correlator in order to receive a chosen image. The resulting masks can be used for security and encryption systems, as the desired image will be received in the output plane only when the two specific phase masks are placed in the $4f$ correlator. Because computation of the two holograms starts from completely random functions, they cannot be reproduced, even if the output image is known. With the same phase mask in the spatial-frequency plane, the system can produce many images in the output by the introduction of different input masks. Therefore, in addition to simple verification, the system can provide information on the identity of the authorized person. Our group is currently working on a similar algorithm for security system implemented in a joint transform correlator (JTC). The expected advantage from a JTC-based security system is the invariance of the system to in-plane shifts of both masks. Thus the JTC can be a proper solution for the problem of misalignment sensitivity of the filter mask in the $4f$ correlator. We hope that the report of this study will be published soon.

References

1. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33,** 1752–1756 (1994).
2. B. Javidi, G. S. Zhang, and J. Li, "Experimental demonstration of the random phase encoding technique for image encryption and security verification," Opt. Eng. **35,** 2506–2512 (1996).
3. B. Javidi and E. Ahouzi, "Optical security system with Fourier plane encoding," Appl. Opt. **37,** 6247–6255 (1998).
4. R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," Opt. Eng. **35,** 2464–2469 (1996).
5. J. Rosen, "Learning in correlators based on projections onto constraint sets," Opt. Lett. **18,** 1183–1185 (1993).
6. H. Stark, ed., *Image Recovery Theory and Application*, 1st ed. (Academic, New York, 1987).
7. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20,** 767–769 (1995).
8. B. Javidi, L. Bernard, and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," Opt. Eng. **38,** 9–19 (1999).
9. B. K. Jennison, J. P. Allebach, and D. W. Sweeney, "Iterative approaches to computer-generated holography," Opt. Eng. **28,** 629–637 (1989).