Introducing secure modes of operation for optical encryption

Thomas J. Naughton,[1,2,*] Bryan M. Hennelly,[1] and Tom Dowling[1]

[1]*Department of Computer Science, National University of Ireland, Maynooth, County Kildare, Ireland*
[2]*University of Oulu, RFMedia Laboratory, Oulu Southern Institute, Vierimaantie 5, 84100 Ylivieska, Finland*
[*]*Corresponding author: tomn@cs.nuim.ie*

Received February 27, 2008; revised July 15, 2008; accepted July 15, 2008;
posted July 31, 2008 (Doc. ID 93219); published September 29, 2008

We analyze optical encryption systems using the techniques of conventional cryptography. All conventional block encryption algorithms are vulnerable to attack, and often they employ secure modes of operation as one way to increase security. We introduce the concept of conventional secure modes to optical encryption and analyze the results in the context of known conventional and optical attacks. We consider only the optical system "double random phase encoding," which forms the basis for a large number of optical encryption, watermarking, and multiplexing systems. We consider all attacks proposed to date in one particular scenario. We analyze only the mathematical algorithms themselves and do not consider the additional security that arises from employing these algorithms in physical optical systems. © 2008 Optical Society of America

OCIS codes: 060.4785, 100.4998, 070.2580, 070.4560.

1. INTRODUCTION

Information security has been receiving increasing attention in recent years. Because optical processes have the distinct advantage of sending 2-D complex data in parallel and carrying out otherwise time costly operations at great speeds, they have found growing importance in data encryption. In [1] an optical encryption scheme is proposed called "double random phase encoding" (DRPE), which involves multiplying by two random phases in the input plane and in the Fourier domain. The authors show that if these random phases are statistically independent white noises, then the encrypted image is also a white noise. The random phase key located in the Fourier plane serves as the only key in this encryption scheme.

The properties of this system and systems like it have been investigated extensively [2–7]. Various other linear optical systems have also been proposed in similar encryption architectures [8–19]. For example, the fractional Fourier transform has been utilized in encryption algorithms in conjunction with random phase keys [8–12] and by randomly shifting sections of the image in some fractional domain [13,14]. The Fresnel transform has also been used with random phase keys [15–18] and with random shifting applied in some Fresnel domain [19]. The most general form of the linear canonical transform, implemented with any arbitrary quadratic phase system, has also been used in an encryption system that uses random phase as a key [19].

The DRPE method has been shown to have application in holographic data storage [20,21]. It has been successfully applied with angular multiplexing [22–25], and it has been observed that this methodology offers an improved performance over traditional angular multiplexing in terms of storage capacity [24] and angular selectivity [25]. This improvement is attributed to cross talk between adjacent images being reduced and has recently been both qualified and quantified using a Wigner-based approach [26].

In recent years there have been a number of proposed attacks on DRPE-type encryption systems [27–32]. In an effort to gain a deeper understanding of this system, and to overcome the vulnerability of DRPE systems to attack, we attempt to investigate the parallels between this optical system and conventional cryptography [33–38]. All textbook conventional computer science encryption systems are vulnerable to attack. One way to counteract this is to use secure modes of operation. In this paper we introduce the concept of modes to optical encryption and analyze the results in the context of known attacks. We consider only DRPE, but consider all attacks proposed to date (as described in Section 3) in one particular scenario. As is usual in cryptanalysis, we consider only key security; we assume there is no security in the mechanism and that any potential attacker will know precisely how the key is used to effect encryption/decryption.

We introduce modes in the following scenario. Consider a sequence of m images that is to be optically encrypted, or equivalently, a stream of data that is very large compared to the input space of the DRPE apparatus. The output corresponding to such an input will be a sequence of encrypted images. The most secure way of encrypting these data is to use a separate encryption key for each image. However, using a separate key for each image is often impractical. In the scenario we describe here, the sender can transmit securely at most one or two phase masks to the receiver before sending the encrypted images over an insecure communication channel. The sender is therefore forced to reuse the same key for each image to be encrypted. What can the sender do? The most straightforward approach is to encrypt each with the same key. However, this is vulnerable to attack. In this paper, we present several modes of operation, of increasing sophis-

tication, that allow the sender some level of defense against the known attacks upon DRPE.

In Section 2 we briefly review the DRPE system, and in Section 3 we present a summary of these attacks on the system that have been proposed in the literature. In Section 4 we discuss the concept of secure modes in conventional cryptography systems and outline a number of suggestions on how the concept of modes can be incorporated into the DRPE optical encryption system. In Section 5 we discuss briefly implementation issues, and we conclude in Section 6.

2. DRPE

The method of DRPE [1] makes use of the optical Fourier transform (OFT). Two phase masks are used in the encryption scheme, which are in the form of two statistically independent white sequences uniformly distributed in [0,1]. We will denote these random functions as k_1 and k_2, which are often displayed on spatial light modulators (SLMs) that can display amplitude and phase information. An optical encryption implementation can be seen in Fig. 1. The scheme works as follows: The input image to be encoded is multiplied by one random phase mask. The resulting complex wave field is optically Fourier transformed using a convex lens, and in the Fourier domain it is multiplied by the second phase mask displayed on a second SLM. The resulting image is again Fourier transformed through the use of a second lens. This is equivalent to a convolution operation, where the encrypted image can be represented by

$$C(x) = E(P(x)), \tag{1a}$$

$$E(P(x)) = \{P(x)\exp[j2\pi k_1(x)]\} * h(x), \tag{1b}$$

$$F\{h(x)\} = \exp[j2\pi k_2(x)]. \tag{1c}$$

The $*$ denotes the convolution operation, $P(x)$ represents the signal to be encrypted (plaintext), $C(x)$ denotes the encrypted image (ciphertext), $E(\,)$ denotes the encryption process that is DRPE, and F denotes the Fourier transform operator. One-dimensional functions are used for simplicity.

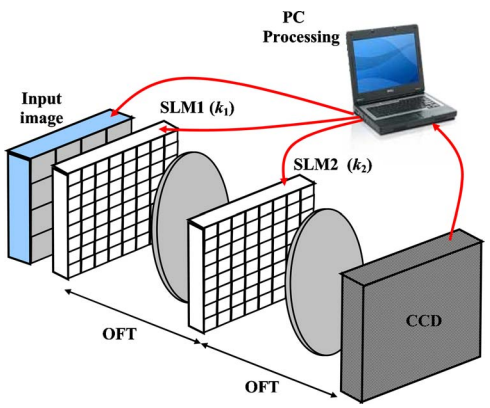

Fig. 1. (Color online) General optical encryption/decryption setup for DRPE. OFT, optical Fourier transform; k, random phase mask represented on a SLM.

The resulting encrypted image, which is complex valued, can be shown to be a stationary white noise [1]. The first random phase mask serves to make the input image white but nonstationary and not encrypted. The second serves to make the image stationary and encoded. Because the encrypted image is complex valued, both the real and imaginary parts are needed to decode the image. In order to record such a wave field (magnitude and phase), we must use holographic interferometric methods [39–43].

Decryption is defined as

$$P(x) = D(C(x)), \tag{2a}$$

$$D(C(x)) = \{C(x) * h(-x)\}\exp[-j2\pi k_1(x)], \tag{2b}$$

where $D(\,)$ denotes decryption. To decrypt we apply the exact inverse of what was done to encrypt the image: First, return to the Fourier domain through the action of a lens. Next, multiply by a phase mask, which is the conjugate of the corresponding phase mask used in the encryption process. A last Fourier transforming lens follows this. In most cases the input image is a real amplitude image. After this last OFT, the resulting wave field will have an amplitude distribution equal to the original image, so holographic techniques are not necessary to capture it. Furthermore, since we are interested only in the amplitude of the image in the output plane, we need not multiply by the conjugate of the first phase mask, since this will have no effect on the amplitude. Thus, we can drop the exponential term in Eq. (2b), and there is only one key in this decryption scheme, the second random phase function, without which, blind decryption is very difficult [6].

The properties of such an encryption–decryption system have been investigated [2–7]. It is worth noting that since the system is linear, it exhibits behavior identical to that of the Fourier transform with regard to additive and multiplicative noise in optical implementations. DRPE has also been extended to use a complex signal as the input to the system instead of an amplitude-based image [4]. Such a system can be shown to have an improvement in robustness to additive noise. However, unlike the case of the input real only image, the first phase mask must be included during decryption and Eq. (2b) must include the exponential term and the final decrypted image must be recorded using interferometric methods.

We note that in DRPE, the first random phase plane serves to make the input image white but nonstationary and not encrypted [1]. The second serves to make the image stationary and encoded. Thus, the random phase key located at the Fourier plane of this system, k_2, serves as the only key in this encryption scheme. In the following sections we attempt to apply the concept of modes of encryption to DRPE. In the next section we discuss a number of attacks that have been proposed in the literature to hack into the DRPE system.

3. EXISTING ATTACKS ON DRPE SYSTEMS

Two classes of attack have been proposed to date on DRPE: one class seeking an exact solution to the phase

masks and the other seeking an approximate solution. The most relevant of the attacks summarized below are listed in Table 1.

A. Exact Solutions

Exact attacks are analytic in nature.

1. Chosen Plaintext Attack

The simplest type of cryptographic attack is the chosen plaintext attack. In this attack the attacker obtains the encrypted version of a plaintext of their choosing and uses the plaintext–ciphertext pair to deduce the encryption key. It has been demonstrated [27,28] that if the attacker can induce a centered [27] or noncentered [28] delta function to be encrypted, then the second phase mask can be found. This is sufficient to decrypt a real-valued plaintext. For convenience, we call this the delta attack. Only a single chosen plaintext–ciphertext pair is required, a real-valued plaintext is assumed, and holographic recording of the output is assumed. The delta attack has a simple defense due to Carnicer *et al.*: simply do not allow delta functions to be encrypted [27]. However, a refinement of this attack, which we call the delta-H attack, allows the delta function to be hidden within any set of innocuous images whose linear combination is a shifted delta function [28]. For the delta-H attack, as few as two chosen plaintext–ciphertext pairs are required and the simple defense to the delta attack is overcome. Simple extensions to the defense (such as subtracting the current plaintext from each previously encrypted plaintext to search for a delta function) will protect against this attack when it is known that the delta function is hidden within only two pairs. However, if the delta function is hidden within the linear combination of an arbitrary sequence of plaintexts, then it will be impractical to check for all possible linear combinations over any subset of previously encrypted plaintexts. Therefore, we regard the delta-H attack as not having been properly defended against by straightforward extensions to the defense of Carnicer *et al.*

Variants of DRPE that employ phase encoding of their DRPE inputs [44] are also susceptible to the delta-H attack [28]. As an extension, Frauel *et al.* [28] have shown that if the second phase mask is known, then one further chosen plaintext–cipertext pair (where the plaintext is an image with constant complex amplitude) will allow the first phase mask to be found, allowing complex-valued plaintexts (including phase-encoded plaintexts) to be decrypted. We call this the delta-C attack.

If only the intensity of the ciphertext in each chosen plaintext–cipertext pair can be measured, but if it is possible to obtain many chosen plaintext–cipertext pairs, Carnicer *et al.* [27] have shown that N pairs can be used to decrypt the N pixels of the second phase mask. In this attack, the plaintexts are composed of delta functions, and we call it the delta-P attack. The delta-P attack can be combined with the delta-C attack to decrypt complex-valued plaintexts. A delta-P-type attack has also been described for Fresnel encryption [29].

2. Known Plaintext Attack

Known plaintext attacks are more sophisticated attacks because it is not necessary for the attacker to choose the particular plaintext(s) to be encrypted; they only need to know their values. Frauel *et al.* [28] have shown that with the knowledge of N linearly independent plaintext images (that constitutes a base of the N-pixel input space) and knowledge of their corresponding ciphertexts, an attacker is able to directly decrypt all other images encrypted with the same masks, where N is the number of pixels in the plaintext. We refer to this attack as the LA1 (linear algebra 1) attack, because its basic step is a matrix inversion. Although it can cope with complex-valued and phase-encoded plaintexts in additional to regular amplitude-encoded plaintexts, its practicality is limited by the fact that for DRPE systems operating over images with N pixels, the attacker must wait for N linearly independent inputs (and their corresponding outputs).

For the same computational cost, one can obtain the same result with only two plaintext–ciphertext pairs. Frauel *et al.* [28] have shown that given two pairs encrypted with the same phase masks, one can construct a system of N linear equations with N unknown variables, where N is the number of pixels in each mask. Solving this system using classical system-solving techniques [such as Gauss elimination or lower triangular–upper triangular (LU) decomposition] gives the first phase mask.

Table 1. List of Attacks on DRPE

Attack	Refs.	Class[a]	Pairs Required	Time[b]	Phase Inputs[c]	Mode[d]	Brief Reminder of Type of Attack
Delta	[27,28]	Ex-Ch	1	O(1)	N	ECB	Centered delta, holographic recording
Delta-H	[28]	Ex-Ch	2	O(N)	Y	CFB	Hidden delta function
Delta-C	[28]	Ex-Ch	3	O(N)	Y	CFB	Obtain both phase keys
Delta-P	[27]	Ex-Ch	N	O(N)	N	CFB	Requires only intensity to be probed
LA1	[28]	Ex-Kn	N	O(N^3)	Y	CFB	Linear algebra: matrix inversion
LA2	[28]	Ex-Kn	2	O(N^3)	Y	CFB	Linear algebra: solve linear system
Delta-P	[27]	Ap-Ch	N	O(N)	N	CFB	Requires only intensity to be probed
SA	[30]	Ap-Kn	1	O(N)	N	OFB	Simulated annealing
PR	[31]	Ap-Kn	1	O(N)	N	OFB	Phase retrieval

[a]Ex/Ap, Exact/Approximate decryption; Ch/Kn, Chosen/Known plaintext.

[b]For the complexity analysis (where N is the number of pixels), we assume that each optical encryption/decryption operation requires just one computation step. Heuristics SA and PR are approximated as requiring a linear number of iterations.

[c]Denotes whether attack can cope with phase-encoded inputs.

[d]The weakest mode that protects against this attack.

Once the first phase mask is known, the second mask can be calculated directly. We refer to this attack as the LA2 (linear algebra 2) attack. The complexity of this attack is $O(N^2)$ in space and $O(N^3)$ in time. For an image with $N = 10^4$ pixels, the masks can be found in approximately 2 h on a desktop computer using Gaussian elimination with back substitution [28]. Again, complex-valued and phase-encoded plaintexts are also susceptible in this attack.

Finally, we note that an attack by Lee *et al.* [32] on an encryption technique for holographic memory that is simpler than DRPE is not considered here.

B. Approximate Solutions

The advantage of using a heuristic to approximate phase mask pixels rather than an analytical technique to determine exact solutions for the pixels is that a heuristic can take considerably less time to run. Furthermore, since the data routinely encrypted by optical encryption are image data, slight errors in the decrypted data can often be tolerated, and so an exact solution is not generally required. The simplest type of attack is a brute force attack in which the key is approximated by trying all in a restricted set of possibilities [28]. It has been shown that this kind of attack is not feasible [6].

1. Chosen Plaintext Attack

The delta-P attack of Carnicer *et al.* [27] can be utilized so that with M plaintext–ciphertext pairs, a subset M of the pixels of the second phase mask can be retrieved. It has been widely shown that DRPE is tolerant to a large number of missing pixels in the phase masks [27,28]. A delta-P-type attack has also been described for Fresnel encryption [29].

2. Known Plaintext Attack

Gopinathan *et al.* [30] describe a known plaintext attack that uses a heuristic to estimate the second phase mask in a DRPE scenario. Their algorithm is given a single plaintext–ciphertext pair. It is assumed that the plaintext is real valued, and so only the second phase mask is sought. They use a simulated annealing algorithm to find a phase mask that decrypts the output with arbitrarily low error. They show that the technique is not guaranteed to return an acceptable solution but can detect when the technique is failing to converge and demonstrate that at most three parallel runs of the technique are required to acceptably decrypt with a probability of 0.9995. Three parallel runs would require approximately 1 h for a 32×32 pixel input, rising to 17 h for a 64×64 pixel input [30].

Peng *et al.* [31] also assume they are in possession of a single plaintext–ciphertext pair (a real-valued plaintext a and a complex-valued encrypted image b). Peng *et al.* [31] observe that the amplitude of the signal immediately before the second phase mask is identical to the amplitude of the Fourier transform B of the encrypted image b. Together, $|B|^2$ and $|a|^2$ constitute a pair of intensity measurements related by a Fourier transform, which can be used to derive the first phase mask using standard phase-retrieval techniques. Once the first phase mask is known, the second mask can be calculated directly. The accuracy with which the first phase mask is found is dependent on both the sophistication of the phase-retrieval algorithm employed and the length of time it is run.

4. CONVENTIONAL MODES OF OPERATION FOR BLOCK ENCRYPTION SYSTEMS

In this section we review the concept of secure modes in modern conventional cryptography for block encryption systems and apply these concepts to DRPE. This will provide a means to overcome the attacks reviewed in the previous section.

A. Modes

Cryptographic block ciphers partition messages into data blocks before transmission. These blocks are then processed, one at a time. Questions arise as to what is the best way to do this and can extra desirable properties be integrated into this procedure. These questions are usually addressed by using standard modes of operation along with the basic cryptographic algorithm. These modes of operation can be used to incorporate nondeterminism into a block cipher algorithm. Nondeterminism is necessary but not always sufficient to protect against modern adaptive cryptographic attacks. Modes of operation can also be used to pad in a more secure way, control error propagation, and transform a block cipher into an arbitrary length stream cipher. Four main modes of operation are described below. A comprehensive account of modes of operation appears in [34]. In this section we attempt to adapt the secure coding schemes developed for conventional cryptography for the DRPE system. There are obvious differences between the mathematical definitions and the physically realizable optical operations. We substitute straightforward compromises in these instances.

B. Notation

We introduce the following notation:

Let $E_k(\cdot)$ denote some encoding scheme in the case of conventional cryptography and a DRPE encryption with some key k in the case of optical encryption.

Let $D_k(\cdot)$ denote the corresponding decoding scheme in the case of conventional cryptography and a DRPE decryption with the key k in the case of optical encryption.

Let P_i denote the ith plaintext image, where $1 \leqslant i \leqslant m$ and where m is the total number of images being encrypted.

Let I_i denote an intermediate image or intermediate text.

Let C_i denote the corresponding ciphertext image.

Let IV denote an initial image value required by some modes of operation.

C. Electronic Codebook Mode

The electronic codebook (ECB) mode is the simplest mode, where blocks are encrypted sequentially,

$$C_i = E_k(P_i), \qquad 1 \leqslant i \leqslant m. \tag{3}$$

Decryption is given by

$$P_i = D_k(C_i), \qquad 1 \leq i \leq m. \tag{4}$$

This is the simplest mode and equates directly to the standard DRPE system. Equations (3) and (4) above can be used to directly represent DRPE encryption and decryption, respectively. A flow chart for encryption and decryption is shown in Fig. 2, and an illustration of encryption is given in Fig. 3(a). We note that the inverse Fourier transform has an almost identical optical implementation to the Fourier transform. Using the defense of Carnicer *et al.* [27], this mode is secure against the delta attack. However, this mode is vulnerable to other attacks because it is deterministic: Multiple images are encrypted sequentially with the same key (k_2 in Fig. 1) so that, for example, if identical plaintexts are encrypted, this results in identical ciphertexts. If the required number of plaintext–ciphertext pairs is obtained, the key can be discovered by exploiting either exact attack or approximate attack sensitivity, as described previously in Section 3. The key can then decrypt the entire sequence as illustrated in Fig. 3(b). [To remove this determinism one would need to introduce some limited form of randomization (usually called pseudo-randomization), as will be explained in the next section, so that the key used for each plaintext is not identical to that used for the subsequent plaintext.] Figure 1 illustrates a physically realizable setup for implementing the DRPE in this and all other modes described in this paper. In this implementation both phase keys are displayed on SLMs.

D. Cipher Block Chaining

This ciphertext from this mode is dependent not only on the plaintext block but also on all previous data blocks as

$$C_0 = IV, \tag{5a}$$

$$C_i = E_k(P_i \oplus C_{i-1}), \qquad 1 \leq i \leq m, \tag{5b}$$

where $\oplus$ denotes a bitwise exclusive or (XOR) operation. Decryption is achieved with Eq. (5a) and

$$P_i = D_k(C_i) \oplus C_{i-1}, \qquad 1 \leq i \leq m. \tag{6}$$

Note that since IV is treated as a ciphertext block, it need not be secret but should change on each encryption session. The receiver should be sent the IV along with the cipertexts in order to decrypt. The result of this chaining is

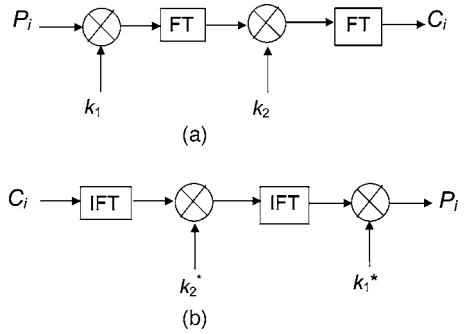

Fig. 2. Flow chart for (a) DRPE encryption E_k and (b) DRPE decryption D_k. FT, Fourier transform; IFT, inverse Fourier transform. The conjugate of the phase key k_2 is used in the decryption process. The symbol * denotes complex conjugation.

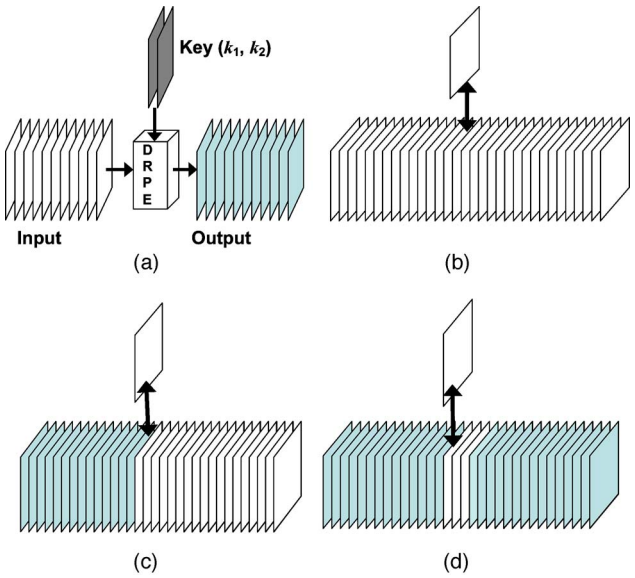

Fig. 3. (Color online) Illustrations of DRPE operation: (a) Sequence of plaintext inputs (in white) is encrypted to ciphertext outputs (shaded). (b) In ECB and CBC modes, if attackers obtain the key they can immediately decrypt the entire sequence. (c) In CFB mode, if attackers approximate the key with a single plaintext–ciphertext pair, only subsequent images can be decrypted because function f_1 is not reversible. (d) In both CFB and OFB modes, careful choice of f_1 can mean that the propagation of errors from an attack that only approximates the key will mean that only a very small number of subsequent images will be decrypted.

that the ciphertext messages are randomized and not deterministic as in the case of ECB. It is also worth noting that although it initially seems so, the cipher block chaining (CBC) mode cannot provide data integrity protection. An attack illustrating this appears in [37].

Since in general we will not be dealing with binary images, we will generalize the $(P_i \oplus C_{i-1})$ operation with any reversible operation, $f(P_i, C_{i-1})$, where its inverse is defined from $P_i = f^{-1}(f(P_i, C_{i-1}), C_{i-1})$. In this case Eqs. (5b) and (6) describing encryption and decryption above are reformulated for DRPE as

$$C_i = E_k(f(P_i, C_{i-1})), \qquad 1 \leq i \leq m, \tag{7}$$

$$P_i = f^{-1}(D_k(C_i), C_{i-1}), \qquad 1 \leq i \leq m. \tag{8}$$

It is clear that the ciphertext depends on the plaintext and all other previous encrypted data blocks. The initial image $C_0 = IV$ is not secret but should change on each session. The ciphertexts are pseudo-randomized. Each encrypted image is used with the next plaintext image to derive the input image on the first SLM. To derive this input we use the reversible function f, which could possibly be implemented electronically or optically. This mode is designed to confuse an attacker. A flow chart for this mode is given in Fig. 4. The setup illustrated in Fig. 1 can be used to implement this mode.

One possible implementation of $f(A, B)$ might be addition of the complex functions, $A + B$. In this case, $f^{-1}(A, B)$ would be given by $A - B$. This could be performed numerically or optically by complex (spatial) superposition of two images. Another possible f could be multiplication. In this

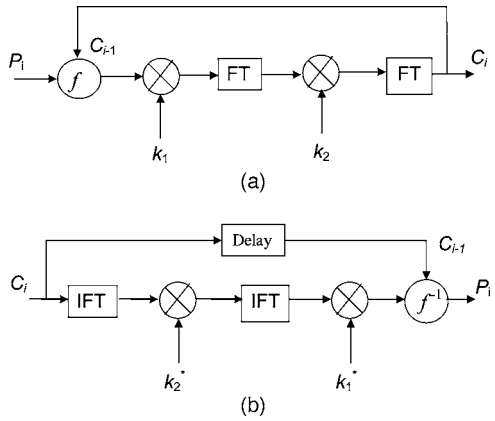

Fig. 4. Flow chart for CBC mode. (a) Encryption, where the two phase mask products and two FTs represent the E_k operation. (b) Decryption, where the two phase mask products and two IFTs represent the D_k operation. The flow chart does not show that at $i=1$, the initial feedback image is C_0=IV.

case, f^{-1} would be given by division. Multiplication could be implemented numerically or optically using an optically addressed SLM. A third possible implementation could be convolution, $f(A,B)=A*B$, where the asterisk denotes the process of convolution. In this case the inverse would be a deconvolution. This could be implemented efficiently in a computer using a fast Fourier algorithm or optically using an OFT and a pair of SLMs. Interestingly, another possible implementation could be a DRPE system, $f(A,B)=E_B(A)$. In this case the inverse function would be $A=D_B(f(A,B))$.

Although initially it might seem that attacks that rely on multiple plaintext–ciphertext pairs are foiled by this optical CBC mode, the reversibility of f means that each of these attacks could be successfully modified. This is because the conventional CBC algorithm is designed to be used with a nonlinear encryption technique. Modified attacks could be mounted as follows. Note that in conventional cryptanalysis we cannot assume that the encryption/decryption methods used are secret; only the key can be considered secret. With one or more plaintext–ciphertext pairs (P_i,C_i) and knowledge of the previous ciphertext in the sequence, an attacker would compute each $I_i=f(P_i,C_{i-1})$ and, using (I_i,C_i) in the role of each plaintext–ciphertext pair, deduce the key k using published techniques [27–31]. With k, the attacker would compute $I_i=D_k(C_i)$ from any unbroken ciphertext encrypted with k and apply f^{-1} to the result to obtain the plaintext.

E. Cipher Feedback Mode

The conventional cipher feedback (CFB) mode is designed to provide additional functionality rather than additional security compared to the previous mode [34]. It provides a way to convert a block cipher into a stream cipher [35] so that it can be more useful for wireless communications, for example. This mode feeds successive bits of ciphertext back as input to the encryption algorithm. However, in this paper we look only at the block cipher variant of conventional CFB, as described in [38]. Although in conventional cryptography there may not be sufficient motivation for a block cipher version of CFB, we show below that in a DRPE interpretation, CFB has a significant advantage over CBC. CFB encryption is defined as

$$I_1 = IV, \tag{9a}$$

$$I_i = C_{i-1}, \qquad 2 \leqslant i \leqslant m, \tag{9b}$$

$$C_i = P_i \oplus E_k(I_i), \qquad 1 \leqslant i \leqslant m, \tag{9c}$$

where the encrypted version of the previous ciphertext is combined using XOR with the next plaintext block. Decryption is defined as combining Eqs. (9a) and (9b) with

$$P_i = C_i \oplus E_k(I_i), \qquad 1 \leqslant i \leqslant m. \tag{10}$$

In this mode the encryption function is also used for decryption. This allows much greater flexibility in the choice of $E_k(\,)$ and includes the use of one-way hash functions. For an account of hash functions, see [36].

In the process of adapting this mode, and in order to free ourselves of the XOR notation, we rewrite the encryption in Eqs. (9b) and (9c) in terms of two functions, f_1 and f_2, as

$$I_i = f_1(I_{i-1},C_{i-1}), \qquad 2 \leqslant i \leqslant m, \tag{11a}$$

$$C_i = f_2(P_i,I_i), \qquad 1 \leqslant i \leqslant m, \tag{11b}$$

where f_1 is irreversible and f_2 is reversible. Similarly, we express decryption by replacing Eq. (11b) with

$$P_i = f_2^{-1}(C_i,I_i), \qquad 1 \leqslant i \leqslant m. \tag{12}$$

The irreversible function f_1 takes the previous ciphertext and the previous key and generates the key with which to encrypt the next plaintext. These are the same two inputs defined for the stream cipher variant of CFB [34]. The reversible function $f_2(P_i,I_i)$ has an inverse defined using $P_i=f_2^{-1}(f_2(P_i,I_i),I_i)$.

For our specific DRPE adaptation, we let DRPE take the place of the reversible f_2 operation. The irreversible f_1 operation can be implemented elsewhere (in optics or electronics). It has been shown [45] that DRPE itself should not be used for the irreversible f_1. In such a scenario, DRPE encryption is defined as

$$I_1 = k_2, \tag{13a}$$

$$I_i = f_1(I_{i-1},C_{i-1}), \qquad 2 \leqslant i \leqslant m, \tag{13b}$$

$$C_i = E_{I_i}(P_i), \qquad 1 \leqslant i \leqslant m, \tag{13c}$$

and DRPE decryption is defined by Eqs. (13a) and (13b) and

$$P_i = D_{I_i}(C_i), \qquad 1 \leqslant i \leqslant m. \tag{14}$$

The choice of the irreversible f_1 function can be arbitrary as long as it takes as input a phase mask and complex-valued image and returns a pure phase mask. In an optical implementation it could utilize a thick semitransparent block with multiple amplitude scatterings placed in front of the illuminated product of the two inputs, and the scattered intensity recorded, where the intensities modulo 2π are considered as phase values for the next key. Numerically, any of the conventional keyed crypto-

graphic hash functions [34,36] such as MD5 or SHA-1 could be adapted for the role.

A flow chart for the CFB mode with DRPE is given in Fig. 5. Again Fig. 1 can be employed as an illustration of a physical implementation of the setup. We begin with the initial Fourier plane phase mask k_2 and encrypt a plaintext image. The resulting ciphertext and k_2 are used as input to some irreversible function f_1 to generate the Fourier plane phase mask to encrypt the next plaintext. In decryption, k_2^* is used to decrypt the first ciphertext, and thereafter each ciphertext is decrypted using the complex conjugate of the output of f_1. The most important aspect of the CFB mode with DRPE is that the encryption key changes for each plaintext. This is similar to the concept of autokeying in conventional symmetric cryptography systems [46].

Because no two plaintext–ciphertext pairs are encrypted using the same key, all exact attacks that require multiple plaintext–ciphertext pairs encrypted with the same key are foiled by this mode. Namely, the chosen plaintext attacks delta-H, delta-C, and delta-P, as well as the known-plaintext attacks LA1 and LA2, are foiled by this mode. Also, delta-P used as an approximation attack is also foiled, as it requires all pairs to be encrypted with the same key. Due to the irreversibility of f_1, it is unlikely that these attacks could be modified in a straightforward manner. However, approximate attack sensitivity remains for this mode, specifically, attacks SA and PR. These attacks require only a single pair to approximate the key. However, since f_1 is not reversible, if one plaintext–ciphertext pair is obtained, only subsequent images can be decrypted and not the whole sequence. This point is illustrated in Fig. 3(c).

Furthermore, a well-chosen irreversible f_1 will be highly sensitive to the key I_i. This is certainly the case with a cryptographic hash function [34,36]. It could be arranged too in an optical implementation by choosing an f_1 that embodied the properties of a chaotic function [47]. By their nature, the approximate attacks SA and PR will find

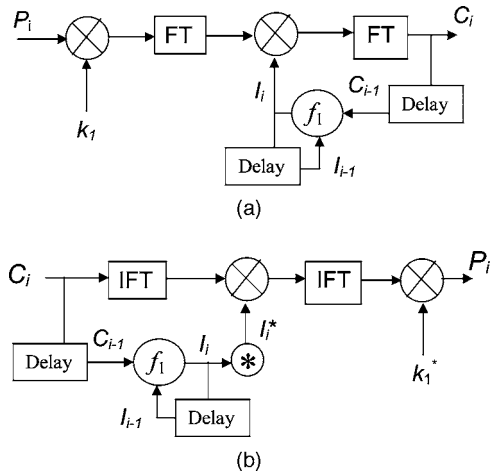

Fig. 5. Flow chart for CFB mode. (a) Encryption, where the two phase mask products and two FTs represent the E_I operation. (b) Decryption, where the two phase mask products and two IFTs represent the D_I operation. Function * denotes the application of complex conjugation. The flow chart does not show that at $i=1$, $I_i=k_2$.

the key with some error. As such, when the attacker passes only an approximated key to f_1, it will either compute the incorrect key for the next ciphertext immediately or else propagate and accumulate the errors so quickly that only a small number of subsequent ciphertexts will be decrypted. This point is illustrated in Fig. 3(d). Unfortunately, errors will propagate for the legitimate decrypter too. With optical systems operating on gray-scale images and incorporating an interferometric measurement technique, one has to allow for the propagation of errors. Of course, the errors will not be as large, because the legitimate user will start with the exact key rather than just an approximated one, but the errors could still be significant for highly nonlinear f_1.

F. Output Feedback Mode

The output feedback (OFB) mode is similar to CFB but differs in the way the feedback is handled. The feedback here happens before the XOR with the plaintext. The feedback circuit forms a finite-state machine with the state determined only by the encryption key of the underlying encryption algorithm. The advantage of this is that propagation errors will affect only one block of ciphertext and will not be amplified as with the other modes. This makes OFB suitable for noisy channels such as in mobile or satellite communications. Encryption is defined as

$$I_1 = IV, \tag{15a}$$

$$I_i = E_k(I_{i-1}), \qquad 2 \leq i \leq m, \tag{15b}$$

$$C_i = P_i \oplus I_i, \qquad 1 \leq i \leq m, \tag{15c}$$

and decryption is defined using Eqs. (15a) and (15b) with

$$P_i = C_i \oplus I_i, \qquad 1 \leq i \leq m. \tag{16}$$

Once again, in order to free ourselves of the XOR notation, we can rewrite Eqs. (15) and (16) in terms of two functions, f_1 and f_2, where f_1 represents E_k and f_2 represents XOR. For conciseness, we do not give these here. Function f_2 is reversible, and f_1 can be reversible or irreversible because the values in Eq. (15b) are never observed directly by the attacker in the attacks under consideration in this paper. Although f_1 can be reversible, it should not be linear; inputs to f_1 should give rise to highly randomized outputs so that an attacker cannot predict the behavior of f_1. As such, for example, DRPE would not be a good choice for f_1 because a small change in the input gives rise to a small change in the output. For our DRPE formulation of the OFB mode, we choose to employ DRPE for f_2 and some arbitrary competent conventional keyed cryptographic hash function [34,36] for f_1. Encryption is defined as

$$I_1 = k_2, \tag{17a}$$

$$I_i = f_1(I_{i-1}), \qquad 2 \leq i \leq m, \tag{17b}$$

$$C_i = E_{I_i}(P_i), \qquad 1 \leq i \leq m, \tag{17c}$$

and decryption is defined by Eqs. (17a) and (17b) and

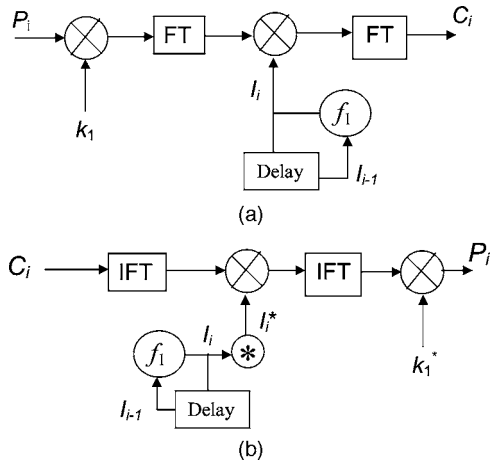

Fig. 6. Flow chart for OFB mode. (a) Encryption, where the two phase mask products and two FTs represent the E_I operation. (b) Decryption, where the two phase mask products and two IFTs represent the D_I operation. Function * denotes the application of complex conjugation. The flow chart does not show that at $i=1$, $I_i=k_2$.

$$P_i = D_{I_i}(C_i), \qquad 1 \leqslant i \leqslant m. \tag{18}$$

A flow chart for the system is given in Fig. 6. Figure 1 illustrates a possible optical implementation. For the first plaintext image we encrypt with the initial Fourier plane phase key k_2. To encrypt subsequent plaintexts i, the most recent Fourier plane key is used as input to hash function f_1 to generate the new Fourier plane key I_i.

The OFB mode foils all exact decryption attacks (delta-H/C/P and LA1/2) and delta-P in an approximation attack, because no two plaintext–ciphertext pairs will have used the same Fourier plane key. The SA and PR approximation attacks will reveal the key from a single plaintext–ciphertext pair, but by their nature they will have some errors in the key. By using a cryptographic hash function for f_1 in the OFB mode, only exact knowledge of the key to an arbitrary resolution will permit one to calculate the next correct key in the sequence. Therefore, successful attacking of one page of cyphertext will not lead to instant decryption of any other pages as illustrated in Fig. 3(d).

From the legitimate decrypter's perspective, the resulting system is more robust to the propagation of error; errors will propagate only if the key is approximated, but not if it is known exactly. The legitimate decrypter will have the key in digital format and will be able to manipulate it digitally without error. Even though the legitimate decrypter may have errors in its optical DRPE setup, these errors will not propagate to, or be amplified in, subsequent ciphertext images. As such, it could be regarded as a form of error correcting [48].

5. DISCUSSION ON IMPLEMENTATION

Optical implementation of any of the modes presented in this paper will have a number of requisites. First, it is necessary that a recorded encrypted image can be digitally recorded and transmitted so that it can be used as a part of a feedback system that is at the heart of many of the modes listed in this paper. Second, it is necessary that the phase masks used in the encryption/decryption system can be quickly changed electronically so that new information can be fed back into these phase masks. This requires the use of addressed SLMs.

The first requisite can be met using digital holography, a means of recording a complex wavefront using a digital camera and a reference beam. In recent years the practical application of digital holography for recording double random phase encoded images has been experimentally validated [41–43]. In [41] the authors describe the first documented experimental digital holographic recording of such an image for secure storage and data transmission. In [42] further experimental results were provided for digital recording of DRPE. This time the input was not a planar data image, rather it was a 3-D object scene. It was shown that different 3-D perspectives and depths could be generated from the digitally recorded encrypted hologram. In [41,42] it was shown that if the phase key was also digitally recorded, decryption could be implemented numerically. In [43] further experiments of digital recording of DRPE images are presented in addition to a correlation-based optical reconstruction process for a real-time display of the digitally encrypted image.

We also note that the use of electrically addressed SLMs for representing phase keys in optical encryption schemes has also been experimentally validated [49]. On this basis we believe that the modes listed in this paper are experimentally possible, though some errors in decryption can be expected due to quantization differences between the recorded image and the SLMs.

As yet, we have no recommendations about how the extra computation for the various modes could be shared between electronic and optical systems and between digital or analog implementations. Of course, all tasks could be conveniently implemented in digital electronics. If one uses electrically addressed SLMs, then the data will be in electronic form at some points in the computation anyway. However, it is worth examining if there are alternative implementation opportunities. The claimed advantages for digital optical computing include reductions in speed, interconnection complexity, and power requirements [50,51], and recent applications that take advantage of information already in an optical representation (such as all-optical packet switching in optical communications [52]) look promising. However, digital optical computing of the form that is prevalent today [52] would be convenient only if the operations are pointwise operations that are to be applied to 1-D arrays of pixels at a time—if there are dependencies between neighboring pixels in multiple dimensions (such as in a 2-D convolution), then a digital optical implementation would not be convenient.

The disadvantages of analog systems for computing include inherent noise and low dynamic range compared to digital representations, which puts fundamental limits on the accuracy achievable. However, if analog optics is already employed for the basic DRPE steps, then one can assume that many of these concerns about analog systems will already have been alleviated or will be less relevant for the application in hand. The analog computation could be performed either electronically or optically. Analog electronics has the same limitation as digital optical computing above—it is not ideally suited to 2-D im-

age processing. Analog optical image processing is a strong contender, as the data are in an optical image representation already. In particular, if optically addressed SLMs are employed, the data might not be in electronic form at the appropriate time. In principle, it has been shown that all possible computations can be performed by analog optics [53,54]. In principle, general-purpose computations can be performed with resources (time and space) equivalent to those required by digital electronics, while many image processing operations can be performed more efficiently. However, care would have to be taken when specifying a very efficient optical implementation for the irreversible function f_1 in CFB and OFB. The most efficient nonlinear operation in analog optics (square law detection) could be susceptible to phase-retrieval techniques and, as has been mentioned, DRPE itself cannot be used as a cryptographic hash function [45]. In particular, the perfect calculation of f_1 in the OFB mode is required in order to avoid the propagation of errors, and so it would be recommended that this step be carried out with digital optics or digital electronics.

6. CONCLUSION

DRPE is vulnerable to both exact decryption and approximate decryption attacks. Secure modes of operation, adopted from conventional cryptography, can be used to foil each of these attacks in the scenario outlined. We adapt these modes for optical implementation with the DRPE system and discuss their impact in terms of added security and propagation of error. ECB is conventional DRPE. CBC adds little security due to its reversibility. CFB exhibits security against all attacks. Equipping CFB to foil approximate decryption attacks requiring only a single plaintext–ciphertext pair results in error propagation for legitimate decrypters of optical systems. OFB is shown to be currently secure against all attacks, in addition to admitting no error propagation for the legitimate decrypter.

ACKNOWLEDGMENTS

We appreciate discussion and ideas from Philippe Réfrégier. We acknowledge funding from Science Foundation Ireland; Enterprise Ireland; the Irish Research Council for Science, Engineering, and Technology; and the European Commission Framework Programme 6 from a Marie Curie Intra-European Fellowship.

REFERENCES

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
2. B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, "Shift tolerance property of an optical double random phase encoding encryption system," Appl. Opt. **39**, 4788–4793 (2000).
3. F. Goudail, F. Bollaro, B. Javidi, and P. Refregier, "Influence of a perturbation in a double random phase encoding system," J. Opt. Soc. Am. A **15**, 2629–2638 (1998).
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, "Optical encryption and the space bandwidth product," Opt. Commun. **247**, 291–305 (2005).
6. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," Appl. Opt. **46**, 6641–6647 (2007).
7. D. S. Monaghan, G. Situ, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Role of phase keys in the double random phase encoding technique: an error analysis," Appl. Opt. **47**, 3808–3816 (2008).
8. G. Unnikrishnan and K. Singh, "Double random fractional Fourier domain encoding for optical security," Opt. Eng. (Bellingham) **39**, 2853–2859 (2000).
9. 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).
10. S. Liu, L. Yu, and B. Zhu, "Optical image encryption by cascaded fractional Fourier transforms with random phase filtering," Opt. Commun. **187**, 57–63 (2001).
11. Y. Zhang, C. H. Zheng, and N. Tanno, "Optical encryption based on iterative fractional Fourier transform," Opt. Commun. **202**, 277–285 (2002).
12. B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," Optik (Stuttgart) **114**, 251–265 (2003).
13. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," Opt. Lett. **28**, 269–271 (2003).
14. N. K. Nischal, G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption using a localized fractional Fourier transform," Opt. Eng. (Bellingham) **42**, 3566–3571 (2004).
15. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762–764 (1999).
16. G. Situ and J. Zhang, "A lensless optical security system based on computer-generated phase only masks," Opt. Commun. **232**, 123–128 (2004).
17. B. M. Hennelly and J. T. Sheridan, "Random phase and shifting encryption in Fresnel domain," Opt. Eng. (Bellingham) **43**, 1–11 (2004).
18. T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," Opt. Eng. (Bellingham) **43**, 2233–2238 (2004).
19. G. Unnikrishnan and K. Singh, "Optical encryption using quadratic phase systems," Opt. Commun. **193**, 51–67 (2001).
20. H. J. Caulfield, D. Psaltis, and G. Sincerbox, *Holographic Data Storage* (Springer-Verlag, 2000).
21. L. Hesselink, S. S. Orlov, and M. C. Bashaw, "Holographic data storage systems," Proc. IEEE **92**, 1231–1280 (2004).
22. B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," Appl. Opt. **36**, 1054–1058 (1997).
23. O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," Appl. Opt. **38**, 7288–7293 (1999).
24. X. Tan, O. Matoba, T. Shimura, and K. Kuroda, "Improvement in holographic storage capacity by use of double-random phase encryption," Appl. Opt. **40**, 4721–4727 (2001).
25. W. C. Su and C. H. Lin, "Enhancement of the angular selectivity in encrypted holographic memory," Appl. Opt. **43**, 2298–2304 (2004).
26. B. M. Hennelly, T. J. Naughton, J. B. McDonald, J. T. Sheridan, G. Unnikrishnan, D. P. Kelly, and B. Javidi, "Spread-space spread-spectrum technique for secure multiplexing," Opt. Lett. **32**, 1060–1062 (2007).
27. 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).
28. 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).
29. X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on

lensless double-random phase encoding in the Fresnel domain," Opt. Lett. **31**, 3261–3263 (2006).
30. 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).
31. 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).
32. H.-Y. Lee, J.-P. Liu, C.-C. Chang, H.-F. Yau, and T.-C. Chang, "The decryption of random phase multiplexing encoding system," Proc. SPIE **5560**, 117–123 (2004).
33. A. A. Vladimirov, K. V. Gavrilenko, and A. A. Mikhailovsky, *Wi-Foo: The Secrets of Wireless Hacking* (Addision, Wesley, 2004).
34. W. Mao, *Modern Cryptography* (Prentice Hall, 2004).
35. W. Stallings, *Cryptography and Network Security*, 4th ed. (Prentice Hall, 2005).
36. W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory* (Prentice Hall, 2001).
37. S. Vaudenay, "Security flaws induced by CBC padding," in *Advances in Cryptology—Proceedings of EUROCRYPT'02, Lecture Notes in Computer Science* (Springer-Verlag, 2002), Vol. 2332, pp. 534–545.
38. B. Schneier, *Applied Cryptography*, 2nd ed. (Wiley, 1996), pp. 200–201.
39. U. Schnars and W. P. O. Juptner, "Digital recording and numerical reconstruction of holograms," Meas. Sci. Technol. **13**, 85–101 (2002).
40. U. Schnars and W. Juptner, *Digital Holography* (Springer, 2005).
41. B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. **25**, 28–30 (2000).
42. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595–6601 (2000).
43. O. Matoba and B. Javidi, "Optical retrieval of encrypted digital holograms for secure real-time display," Opt. Lett. **27**, 321–323 (2002).
44. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A **16**, 1915–1927 (1999).
45. G. Situ, D. S. Monaghan, T. J. Naughton, J. T. Sheridan, G. Pedrini, and W. Osten, "Collision in double random phase encoding," Opt. Commun. **281**, 5122–5125 (2008).
46. R. Anderson, *Security Engineering*, 2nd ed. (Wiley, 2008).
47. S. H. Strogatz, *Nonlinear Dynamics and Chaos* (Perseus Books, 2001).
48. A. Burnett, F. Byrne, T. Dowling, and A. Duffy, "A biometric identity based signature scheme," Int. J. Netw. Secur. **5**, 317–326 (2007).
49. P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," Opt. Lett. **25**, 566–568 (2000).
50. A. Huang, "Architectural considerations involved in the design of an optical digital computer," Proc. IEEE **72**, 780–786 (1984).
51. A. A. Sawchuk and T. C. Strand, "Digital optical computing," Proc. IEEE **72**, 758–779 (1984).
52. H. J. S. Dorren, M. T. Hill, Y. Liu, N. Calabretta, A. Srivatsa, F. M. Huijskens, H. de Waardt, and G. D. Khoe, "Optical packet switching and buffering by using all-optical signal processing methods," J. Lightwave Technol. **21**, 2–12 (2003).
53. T. J. Naughton, "Continuous-space model of computation is Turing universal," Proc. SPIE **4109**, 121–128 (2000).
54. D. Woods and T. J. Naughton, "An optical model of computation," Theor. Comput. Sci. **334**, 227–258 (2005).