On the Security of Optical Ciphers Under the Architecture of Compressed Sensing Combining with Double Random Phase Encoding

Chen, Junxin; Zhang, Yushu; Zhang, Leo Yu

Published in:
IEEE Photonics Journal

Published: 01/08/2017

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.1109/JPHOT.2017.2716961

Publication details:
Chen, J., Zhang, Y., & Zhang, L. Y. (2017). On the Security of Optical Ciphers Under the Architecture of Compressed Sensing Combining with Double Random Phase Encoding. *IEEE Photonics Journal*, *9*(4), [7802611]. https://doi.org/10.1109/JPHOT.2017.2716961

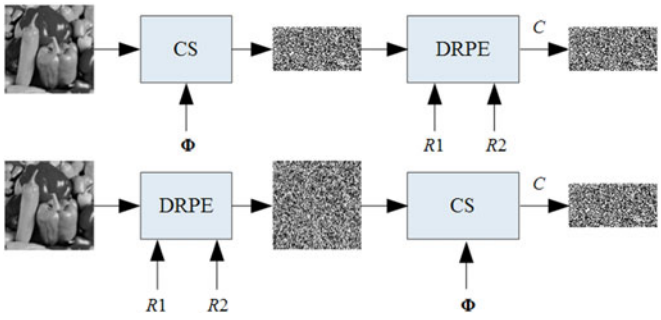
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

On the Security of Optical Ciphers Under the Architecture of Compressed Sensing Combining With Double Random Phase Encoding

Volume 9, Number 4, August 2017

Junxin Chen
Yushu Zhang, ***Member, IEEE***
Leo Yu Zhang, ***Member, IEEE***



DOI: 10.1109/JPHOT.2017.2716961
1943-0655 © 2017 IEEE

IEEE photonics SOCIETY

IEEE

On the Security of Optical Ciphers Under the Architecture of Compressed Sensing Combining With Double Random Phase Encoding

Junxin Chen,[1] **Yushu Zhang,**[2,3] ***Member, IEEE*,**
and Leo Yu Zhang,[4,5] ***Member, IEEE***

[1]Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110169, China
[2]School of Information Technology, Deakin University, Burwood, Vic. 3125, Australia
[3]School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China
[4]School of Information Technology, Jinan University, Guangzhou, 510632, China
[5]Department of Electronic Engineering, City University of Hong Kong, Kowloon, Hong Kong 999077

DOI:10.1109/JPHOT.2017.2716961

Manuscript received May 3, 2017; revised June 6, 2017; accepted June 13, 2017. Date of publication June 26, 2017; date of current version June 29, 2017. This work was supported in part by the National Natural Science Foundation of China under Grants 81671773, 61672146, and 61605025, and in part by the Fundamental Research Funds for the Central Universities under Grants N151904002 and N162410002-4. Corresponding author: Leo Yu Zhang (leocityu@gmail.com).

Abstract: This work investigates the security of optical ciphers integrating compressed sensing (CS) with double random phase encoding. Theoretical analysis demonstrates that the combined system, regardless of the implementation order of the two procedures, can be normalized as a single CS projection process, whose equivalent measurement matrix can be recovered by plaintext attack. The proved restricted isometry property of the equivalent measurement matrices further renders the adversary great convenience to recover the plaintext with only a single-step ℓ_1 optimization. Computer simulations are also carried out for verification.

Index Terms: Imaging systems, optical encryption and authentication.

1. Introduction

In the past decades, optical information cryptosystems have been widely studied with the dramatic increase in the criticality of information security. Among them, double random phase encoding (DRPE) receives tons of attention since its first appearance in [1]. Originating from the intrinsic linear feature, DRPE was found vulnerable against various attacks, such as the chosen-ciphertext attack [2], known-plaintext attack [3] and the chosen-plaintext attack [4]. In [5], a simple whereas more effective chosen-plaintext attack is proposed, which further reveals the vulnerability of DRPE. Regarding the security loophole of the basic design, enhanced DRPE variants have been consequently developed. In [6]–[8], DRPE has been respectively extended to fractional Fourier transform, gyrator transform and Fresnel domains, where the transformation parameters can serve as additional keys. Some other strategies, such as mixed phase-amplitude encoding

[9], phase truncation Fourier transform [10], pixel randomization processing [11], [12], photon-counting [13], coherent diffraction imaging [14], random sampling [15], [16], and phase retrieval [17], [18] are also employed to build optical security systems. On the other hand, compressed sensing (CS) [19]–[21] that emerges as a revolutionary signal acquisition technique has also received extensive research attention in the past few years. Leveraging the fact that natural signals are either compressible or sparse, CS theory demonstrates that such signals can be faithfully reconstructed from a small set of measurements with the sample rate much less than that required by Nyquist-Shannon sample theorem. Exploiting CS for security purpose was firstly outlined in [22], which demonstrates that the measurement vector obtained from the random linear projection can be regarded as the ciphertext with the measurement matrix acts as the secret key. From this sense, the CS can be considered as a variant of symmetric cipher that is computation secure under brute-force attack and ciphertext-only attack [22], [23], whereas vulnerable to plaintext attacks [24], [25].

The concatenation of CS and DRPE seems reasonable and inevitable as the combined system enjoys complete optical implementation and substantial data volumn reduction. Moreover, it is believed that the secrecy of DRPE further enhances the security of CS, and vice visa [26]–[29]. In [26], [27], researchers proposed to first compressively sample the plaintext and then adopt DRPE to further encrypt the measurements, whereas cryptosystems with DRPE-then-CS architecture were developed in [28], [29]. Despite the fact that there is an increasing popularity of designing optical cryptosystems by integrating DRPE with CS [26]–[29], there is no known formal cryptanalysis work studying the security level of these paradigms.

Throughout the previous achievements, the linearity of ciphers under the general architecture of combining DRPE with CS is not difficult to be observed, whereas the specific encryption formulas of such cryptosystems as well as how to recover the plaintext from the encryption matrix has not been mathematically given out. This the primary consideration of this study. Our contributions can be summarized as: 1) the equivalent form of DRPE is deduced out with the help of some properties of the Kronecker product, the linearity and vulnerability of DRPE is intuitively exposed; 2) cryptanalysis demonstrates that both the combined systems can be ultimately normalized as CS processes, and the equivalent measurement matrices could be obtained via plaintext attack; 3) the restricted isometry property (RIP) performance of the equivalent encryption matrices are further proved, which reveals that the decryption (breaking) of both the cryptosystems can be relaxed to a single ℓ_1 optimization in the event that the equivalent encryption matrices have been obtained by plaintext attack. Computer simulations have also been performed to validate the cryptanalysis achievement.

The remainder of this paper is organized as follows. In Section II, reviews of CS and DRPE are presented, cryptanalysis and simulation results are given out in Section III. Finally, conclusions will be drawn in the last section.

2. Reviews

2.1. Notations

In this paper, a lowercase and bold letter is reserved for a vector, a capital and bold letter for a matrix. A lowercase letter may be used to represent the entries of a vector or a matrix, or a variable, whereas a capital letter always denotes a constant. We adopt the 'vec' command as the vectorization operation that reshapes a matrix to a vector by stacking its columns. That is, $\mathbf{X} = [\mathbf{x}^1; \mathbf{x}^2; \cdots; \mathbf{x}^N] = \{x_{i,j}\}_{i=1,j=1}^{M,N} = \{x_{1,1}, \cdots, x_{M,1}; x_{1,2}, \cdots, x_{M,2}; \cdots; x_{1,N}, \cdots, x_{M,N}\}$ represents the $2D$ primary image and $\mathbf{x} = \text{vec}(\mathbf{X}) = [x_{1,1}, \cdots, x_{M,1}, x_{2,1}, \cdots, x_{M,N}]^T$ illustrates its vectorized version.

Besides, the superscript T is denoted as the transpose of a matrix, superscript $*$ as its conjugate, and the superscript H as the conjugate transpose, i.e., $\mathbf{X}^H = \mathbf{X}^{*T}$. The subscript always demonstrates the dimension of the Fourier matrix, or the coordinate of a matrix entry. We use $\cdot$ as the point-by-point product of two matrices.

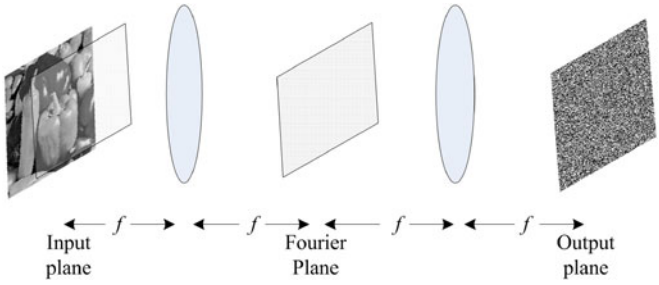


Fig. 1. Principle of double random phase encoding.

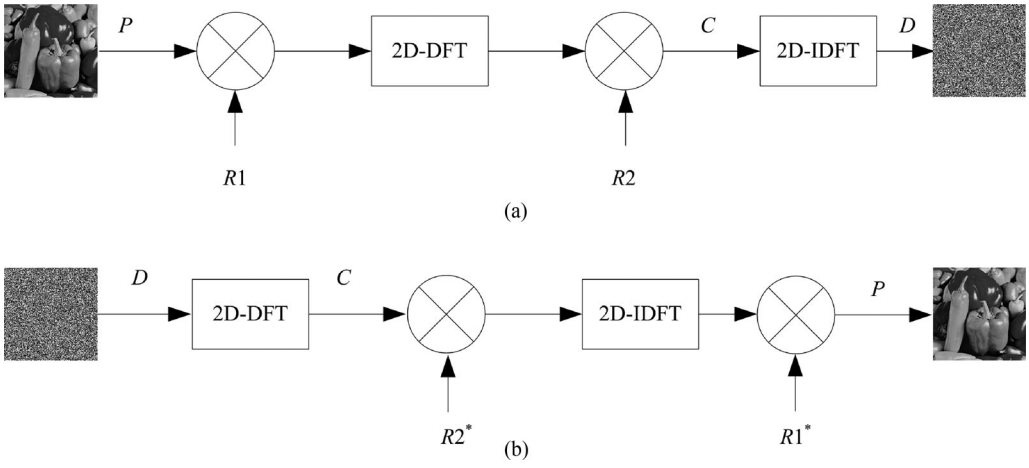


Fig. 2. The block diagrams of DRPE: (a) encryption process, (b) decryption process.

2.2. Double Random Phase Encoding

The principle of DRPE is well-known in optical image encryption field. As illustrated in Fig. 1, DRPE is performed on 4f optical system to encrypt the plaintext into stationary white noise. Fig. 2(a) sums up the encryption operations of DRPE, while Fig. 2(b) demonstrates the decryption procedure. They are respectively written as Eqs. (1) and (2), where $\mathcal{F}$ represents the Fourier Transform (FT) while $\mathcal{F}^{-1}$ is the inverse Fourier transform (IFT). The random phase masks **R1** and **R2** consist of the secret key of DRPE.

$$\mathbf{C} = \mathcal{F}^{-1}(\mathbf{R2} \cdot \mathcal{F}(\mathbf{X} \cdot \mathbf{R1})). \tag{1}$$

$$\mathbf{X} = \mathcal{F}^{-1}(\mathcal{F}(\mathbf{C}) \cdot \mathbf{R2}^{*}) \cdot \mathbf{R1}^{*}. \tag{2}$$

2.3. Compressed Sensing

The CS is originally developed as a revolutionary data acquisition technique that exploits the sparsity or compressibility. For a 1D discrete signal $\mathbf{x} = (x_1, x_2, \cdots, x_N)^T$, $\mathbf{x}$ is said to be K-sparse if $\mathbf{x}$ can be well approximated using only K coefficients under some linear transform $\mathbf{x} = \Psi\mathbf{s}$, where Ψ is the sparsifying basis and $\mathbf{s}$ is the transform coefficient vector with at most $K \ll N$ (significant) nonzero entries. The CS measures signal via the following linear projection,

$$\mathbf{y} = \Phi\mathbf{x} = \Phi\Psi\mathbf{s} = \Theta\mathbf{s}, \tag{3}$$

where $\mathbf{y}$ is the measurement vector with $K \ll N$ entries, Φ represents the $M \times N$ measurement matrix, and Θ is the sensing matrix. For 2D or high-dimensional signals, they can be vectorized to

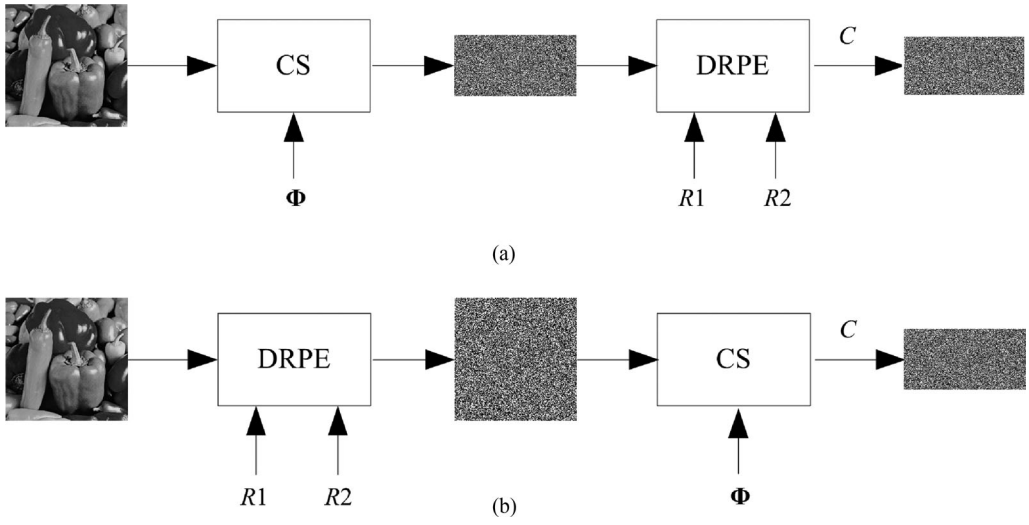


Fig. 3. The combination of CS and DRPE: (a) the C-D architecture, (b) the D-C architecture.

$1D$ format by stacking their columns. The CS theory implies that **x** can be faithfully recovered with overwhelming probability from only $M = O(K \log N)$ measurements, in the case that Θ satisfies the restricted isometry property (RIP) [20]. In such scenarios, the reconstruction of **x** can be preceded by solving the following ℓ_1-norm minimization problem:

$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \mathbf{y} = \Theta\mathbf{s}. \tag{4}$$

Popular matrices families that satisfy RIP including Gaussian and Bernoulli ensembles with $K = O(k \log M)$ rows, which are well known as it is universally incoherent with popular orthonormal sparsifying bases. For example, if Φ is a random matrix of Gaussian entries and Ψ is an arbitrary orthonormal sparsifying basis, the resultant sensing matrix in the transform domain $\Theta = \Phi\Psi$ is also a Gaussian matrix, and hence satisfy RIP requirements [30]. Here we note that all the previous proposals focus on the concatenation of CS and DRPE work with RIP.

2.4. DRPE Combining With CS

Cryptosystems integrating CS with DRPE can be divided into two types with respect to the implementation order of these two procedures. The first type is with the architecture of CS followed by DRPE (abbreviated as C-D), i.e., the plaintext is firstly compressively sampled and subsequently encrypted using DRPE, as illustrated in Fig. 3(a). Referring to Eqs. (1)–(3), the encryption process can be summed as Eq. (5).

$$\begin{aligned} \mathbf{y} &= \text{vec}(\mathbf{Y}) = \Phi\text{vec}(\mathbf{X}) = \Phi\mathbf{x} \\ \mathbf{D} &= \mathcal{F}^{-1}(\mathbf{R2} \cdot \mathcal{F}(\mathbf{Y} \cdot \mathbf{R1})) \\ \mathbf{c} &= \text{vec}(\mathbf{D}). \end{aligned} \tag{5}$$

The latter combination pattern is to perform CS following DRPE, denoted as D-C, shown in Fig. 3(b). Analogously, the encryption process can be described as Eq. (6).

$$\begin{aligned} \mathbf{D} &= \mathcal{F}^{-1}(\mathbf{R2} \cdot \mathcal{F}(\mathbf{X} \cdot \mathbf{R1})) \\ \mathbf{c} &= \Phi\text{vec}(\mathbf{D}). \end{aligned} \tag{6}$$

For ciphers with C-D or D-C architecture, random phase masks **R1** and **R2** of DRPE, the measurement matrix Φ of CS jointly consist of the secret key of the concatenated cryptosystem. At the

decoder side, the decryption should observe a two-step separate operation. Taking C-D scheme as an example, the ciphertext should be firstly decrypted by the DRPE decoder and then reconstructed by ℓ_1 optimization, i.e.,

$$\mathbf{Y} = \mathcal{F}^{-1}(\mathcal{F}(\mathbf{C}) \cdot \mathbf{R2}^*) \cdot \mathbf{R1}^*$$
$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \mathbf{y} = \text{vec}(\mathbf{Y}) = \Theta\mathbf{s}.$$

3. Cryptanalysis

3.1. Preliminaries

Definition 1: The $\mathbf{F}_N$ is defined as the Fourier matrix which can convert the DFT of a length$-N$ signal through matrix multiplication, i.e., $DFT(x) = \mathbf{F}_N x$. The formula of $\mathbf{F}_N$ is described in Eq. (7) where $w = e^{-2\pi i/N}$ is a primitive Nth root of unity [31].

$$\mathbf{F}_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & w^3 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & w^6 & \cdots & w^{2(N-1)} \\ 1 & w^3 & w^6 & w^9 & \cdots & w^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & w^{3(N-1)} & \cdots & w^{(N-1)(N-1)} \end{bmatrix}. \tag{7}$$

Property 1: Both of the Fourier matrix $\mathbf{F}_N$ and its conjugate transpose $\mathbf{F}_N^H$ are symmetric and unitary, i.e., Eqs. (8) and (9) always hold [31].

$$\mathbf{F}_N = \mathbf{F}_N^T. \tag{8}$$
$$\mathbf{F}_N^{-1} = \mathbf{F}_N^H = \mathbf{F}_N^{HT}. \tag{9}$$

Proof: The property is straightforward and hence not presented in detail. ■

Theorem 1: With the definition of Fourier matrix, the 2D $M \times N$ DFT and IDFT can be respectively described as Eqs. (10) and (11) [31].

$$\mathcal{F}(\mathbf{P}_{M\times N}) = \mathbf{F}_M \mathbf{P}_{M\times N} \mathbf{F}_N. \tag{10}$$
$$\mathcal{F}^{-1}(\mathbf{P}_{M\times N}) = \mathbf{F}_M^H \mathbf{P}_{M\times N} \mathbf{F}_N^H. \tag{11}$$

Property 2: Let $\mathbf{P}$ and $\mathbf{R}$ be 2D $M \times N$ matrix, it is found that Eq. (12) always holds, where diag(vec($\mathbf{R}$)) is the $MN \times MN$ diagonal matrix with entries are vec($\mathbf{R}$) from the upper-left to the lower-bottom corner.

$$\text{vec}(\mathbf{P} \cdot \mathbf{R}) = \text{vec}(\mathbf{R} \cdot \mathbf{P}) = \text{diag}(\text{vec}(\mathbf{R}))\text{vec}(\mathbf{P}). \tag{12}$$

Proof: Let's proof vec($\mathbf{P} \cdot \mathbf{R}$) as an example. Mathematically, $\mathbf{P} \cdot \mathbf{R}$ can be written as

$$\mathbf{P} \cdot \mathbf{R} = \begin{bmatrix} p_{1,1}r_{1,1} & p_{1,2}r_{1,2} & \cdots & p_{1,N}r_{1,N} \\ p_{2,1}r_{2,1} & p_{2,2}r_{2,2} & \cdots & p_{1,N}r_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ p_{M,1}r_{M,1} & p_{M,2}r_{M,2} & \cdots & p_{M,N}r_{M,N} \end{bmatrix},$$

then we obtain vec($\mathbf{P} \cdot \mathbf{R}$) $= \{p_{1,1}r_{1,1}, p_{2,1}r_{2,1}, \cdots, p_{M,1}r_{M,1}, p_{2,1}r_{2,1}, p_{2,2}r_{2,2}, \cdots p_{M,N}r_{M,N}\}^T$. Obviously,

$$\text{diag}(\text{vec}(\mathbf{R})) = \begin{bmatrix} r_{1,1} & 0 & 0 & 0 \\ 0 & r_{2,1} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & r_{M,N} \end{bmatrix},$$

and $\text{vec}(\mathbf{P}) = \{p_{1,1}, p_{2,1}, \cdots, p_{M,1}, p_{2,1}, \cdots p_{M,N}\}^T$. Accordingly, we can get

$$\text{diag}(\text{vec}(\mathbf{R}))\text{vec}(\mathbf{P}) = \{p_{1,1}r_{1,1}, p_{2,1}r_{2,1}, \cdots, p_{M,1}r_{M,1}, p_{2,1}r_{2,1}, p_{2,2}r_{2,2}, \cdots p_{M,N}r_{M,N}\}^T.$$

Proof over. ■

Definition 2: If $\mathbf{A}$ is an $M \times N$ matrix and $\mathbf{B}$ is a $P \times Q$ matrix, then the Kronecker product $\mathbf{A} \otimes \mathbf{B}$ is the $MP \times NQ$ block matrix [32]:

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{1,1}\mathbf{B} & \cdots & a_{1,N}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{M,1}\mathbf{B} & \cdots & a_{M,N}\mathbf{B} \end{bmatrix}. \tag{13}$$

Property 3: $(\mathbf{A} \otimes \mathbf{B})^H = \mathbf{A}^H \otimes \mathbf{B}^H$.

Property 4: $(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = (\mathbf{AC}) \otimes (\mathbf{BD})$.

Theorem 2: Supposed that $\mathbf{C} = \mathbf{AXB}$, it has $\text{vec}(\mathbf{C}) = \text{vec}(\mathbf{AXB}) = (\mathbf{B}^T \otimes \mathbf{A})\text{vec}(\mathbf{X})$.

The particular description and proof of properties 3–4 and theorem 2 can be found in [32].

3.2. Equivalent of the Ciphertext

Firstly, let us consider the equivalent form of DRPE, as described in Eq. (1). Taking Eqs. (10) and (11) into Eq. (1), we can get

$$\mathbf{C} = \mathbf{F}_M^H(\mathbf{R2} \cdot \mathbf{F}_M(\mathbf{X} \cdot \mathbf{R1})\mathbf{F}_N)\mathbf{F}_N^H.$$

Employing Theorem 2, we obtain

$$\begin{aligned} \text{vec}(\mathbf{C}) &= \text{vec}(\mathbf{F}_M^H(\mathbf{R2} \cdot \mathbf{F}_M(\mathbf{X} \cdot \mathbf{R1})\mathbf{F}_N)\mathbf{F}_N^H) \\ &= (\mathbf{F}_N^{HT} \otimes \mathbf{F}_M^H)\text{vec}(\mathbf{R2} \cdot \mathbf{F}_M(\mathbf{X} \cdot \mathbf{R1})\mathbf{F}_N). \end{aligned}$$

Considering Properties 1 and 2,

$$\begin{aligned} \text{vec}(\mathbf{C}) &= (\mathbf{F}_N^{HT} \otimes \mathbf{F}_M^H)\text{vec}(\mathbf{R2} \cdot \mathbf{F}_M(\mathbf{X} \cdot \mathbf{R1})\mathbf{F}_N) \\ &= (\mathbf{F}_N^H \otimes \mathbf{F}_M^H)\text{diag}(\text{vec}(\mathbf{R2}))\text{vec}(\mathbf{F}_M(\mathbf{X} \cdot \mathbf{R1})\mathbf{F}_N). \end{aligned}$$

Again, Theorems 1 and 2 and Properties 2 and 3 are introduced for further deduction, we can obtain

$$\begin{aligned} \text{vec}(\mathbf{C}) &= (\mathbf{F}_N^H \otimes \mathbf{F}_M^H)\text{diag}(\text{vec}(\mathbf{R2}))\text{vec}(\mathbf{F}_M(\mathbf{X} \cdot \mathbf{R1})\mathbf{F}_N) \\ &= (\mathbf{F}_N^H \otimes \mathbf{F}_M^H)\text{diag}(\text{vec}(\mathbf{R2}))(\mathbf{F}_N^T \otimes \mathbf{F}_M)\text{vec}(\mathbf{X} \cdot \mathbf{R1}) \\ &= (\mathbf{F}_N^H \otimes \mathbf{F}_M^H)\text{diag}(\text{vec}(\mathbf{R2}))(\mathbf{F}_N^T \otimes \mathbf{F}_M)\text{diag}(\text{vec}(\mathbf{R1}))\text{vec}(\mathbf{X}) \\ &= (\mathbf{F}_N \otimes \mathbf{F}_M)^H\text{diag}(\text{vec}(\mathbf{R2}))(\mathbf{F}_N \otimes \mathbf{F}_M)\text{diag}(\text{vec}(\mathbf{R1}))\text{vec}(\mathbf{X}). \end{aligned}$$

Then, we can get equivalent form of the DRPE ciphertext, as demonstrated in Eq. (14), where $\mathbb{F}$ is the Kronecker product of $\mathbf{F}_N$ and $\mathbf{F}_M$, $\mathbb{R}\mathbf{1} = \text{diag}(\text{vec}(\mathbf{R1}))$, $\mathbb{R}\mathbf{2} = \text{diag}(\text{vec}(\mathbf{R2}))$, and $\mathbf{T}$ is defined as the product of $\mathbb{F}^H\mathbb{R}\mathbf{2}\mathbb{F}\mathbb{R}\mathbf{1}$, respectively. They are all with size $MN \times MN$, with the size of $\mathbf{X}$ is $M \times N$ and will be vectorized to $\mathbf{x}$ with size $MN \times 1$.

$$\mathbf{c} = \text{vec}(\mathbf{C}) = \mathbb{F}^H\mathbb{R}\mathbf{2}\mathbb{F}\mathbb{R}\mathbf{1}\mathbf{x} = \mathbf{T}\mathbf{x}. \tag{14}$$

For C-D architecture, the plaintext is firstly compressively sampled, the measurements will be further encrypted by DRPE. According to the Eqs. (5) and (14), the ciphertext of the C-D scheme can be described as follows.

$$\mathbf{c1} = \text{vec}(\mathbf{C1}) = \mathbf{T}\Phi\mathbf{x} = \mathbf{T}\Phi\Psi\mathbf{s}. \tag{15}$$

Similarly, we can draw the ciphertext with D-C architecture, as shown in Eq. (16).

$$\mathbf{c2} = \text{vec}(\mathbf{C2}) = \Phi\mathbf{T}\mathbf{x} = \Phi\mathbf{T}\Psi\mathbf{s}. \tag{16}$$

3.3. RIP Performance

As mentioned in Section II-C, all the C-D and D-C schemes work with RIP. Here, we illustrate that matrix $\mathbf{T}\Phi$ in Eq. (15), and $\Phi\mathbf{T}$ in Eq. (16) also satisfy the RIP with same order. In this way, the decryption of the concatenated systems (C-D or D-C encryption) can be unified to a single step ℓ_1 optimization procedure, as described in Eq. (17) for C-D scheme and Eq. (18) for D-C cryptosystem, respectively. In other words, the complete cascaded DRPE and CS operations can be normalized as an equivalent CS procedure, with $\mathbf{T}\Phi$ and $\Phi\mathbf{T}$ serve as the equivalent measurement matrices and hence secret keys of the C-D and D-C schemes, respectively.

$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \mathbf{c1} = \mathbf{T}\Phi\Psi\mathbf{s}. \tag{17}$$

$$\min \|\mathbf{s}\|_1 \quad \text{s.t. } \mathbf{c2} = \Phi\mathbf{T}\Psi\mathbf{s}. \tag{18}$$

To begin with, the definition of RIP is briefly reviewed here.

Definition 3: A matrix Φ of size $M \times N$ is said to satisfy the restricted isometry property of order K if there exists a constant $\delta_k \in (0, 1)$ such that

$$(1 - \delta_K)\|\mathbf{s}^{(\mathbf{T})}\|_2^2 \leq \|\Phi^{(T)}\mathbf{s}^{(T)}\|_2^2 \leq (1 + \delta_K)\|\mathbf{s}^{(T)}\|_2^2 \tag{19}$$

holds for all column indices sets T with $\#T < K$ where $\Phi^{(T)}$ is a $M \times \#T$ matrix composed of the columns indexed by T, $\mathbf{s}^{(\mathbf{T})}$ is a vector obtained by retaining only the entries indexed by T and $\|\cdot\|_2$ denotes the ℓ_2 norm of a vector [33].

Roughly speaking, a matrix satisfies RIP requirement roughly retains the energy of the original signal during subspace projection. Thus, the conclusion that $\mathbf{T}\Phi$ satisfy the same RIP order as Φ can be drawn after realizing that $\mathbf{T}$ is a unitary matrix, which is energy-preserving. The detailed proof is given in Property 5.

Property 5: If Φ satisfies RIP requirement with order K, then $\mathbf{T}\Phi$ satisfies RIP requirement with the same order.

Proof: To prove this, it is only required to prove $\mathbf{T}$ is a unitary matrix since

$$\|\mathbf{T}\Phi\mathbf{s}\|_2 = \|\Phi\mathbf{s}\|_2$$

holds true if $\mathbf{T}$ is unitary. Referring to the previous statement that $\mathbf{T}$ is defined as $\mathbf{T} = \mathbb{F}^H\mathbb{R}\mathbf{2}\mathbb{F}\mathbb{R}\mathbf{1}$, where $\mathbb{F}$ is the Kronecker product of $\mathbf{F}_N$ and $\mathbf{F}_M$. Considering Properties 3 and 4, we can get

$$\begin{aligned}\mathbb{F}\mathbb{F}^H &= (\mathbf{F_N} \otimes \mathbf{F_M})(\mathbf{F_N} \otimes \mathbf{F_M})^H \\ &= (\mathbf{F_N} \otimes \mathbf{F_M})(\mathbf{F}_N^H \otimes \mathbf{F}_M^H) \\ &= (\mathbf{F_N}\mathbf{F}_N^H) \otimes (\mathbf{F_M}\mathbf{F}_M^H) \\ &= I \otimes I = I.\end{aligned}$$

Hence, we come to the conclusion that $\mathbb{F}$ is unitary. Besides, $\mathbb{R}\mathbf{1}$ and $\mathbb{R}\mathbf{2}$ are constructed by phase-only matrix, and certainly are unitary. Then we can consequently obtain

$$\mathbf{T}\mathbf{T}^H = (\mathbb{F}^H\mathbb{R}\mathbf{2}\mathbb{F}\mathbb{R}\mathbf{1})(\mathbb{F}^H\mathbb{R}\mathbf{2}\mathbb{F}\mathbb{R}\mathbf{1})^H = I.$$

Hence completes the proof. ■

3.4. Plaintext Attack

As proved above, the cascaded encryption systems can be ultimately viewed as CS projection procedures, whose equivalent measurement matrices are deduced in Eqs. (17) and (18) respectively for C-D and D-C schemes. The kernel of the attack converts to the recovery of the equivalent matrices. From mathematical perspective, one can observe that if $MN \times MN$ identity matrix is imported as the plaintext, the equivalent keys can be one-stepped retrieved through Eqs. (15) and (16). However, the actual input is an $M \times N$ image $\mathbf{X}$ (vector $\mathbf{x}$ with size $MN \times 1$). In practice, the attack can be launched using MN independent plaintexts, i.e., $\mathbf{x}_i = \{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_i, \cdots, \mathbf{x}_{MN}\}$. For

example, $\mathbf{x}_i$ can be one column of the $MN \times MN$ identity matrix, and its ciphertext $\mathbf{y}_i$ is therefore the corresponding column of the equivalent keys. In short, chosen-plaintext attack (CPA) requires MN plaintexts. After the retrieval of secret matrices, which has been proved to be a RIP matrix, a single-step optimization as illustrated in Eqs. (17) or (18) is sufficient to recover the any further encryption results of C-D and D-C cryptosystems, respectively.

It should be noted that, the assumption of CPA is strong since the selected $\mathbf{x}_i$ appears suspicious to the authorized users (or the C-D/D-C encryption machine), so they may deny the encryption service. Alternatively, due to the linearity of the C-D and D-C design, other two plaintexts can be employed if they satisfy

$$\mathbf{x}_i = \mathbf{x}_i^1 - \mathbf{x}_i^2,$$

since their corresponding ciphertext $\mathbf{y}_i^1$ and $\mathbf{y}_i^2$ satisfy

$$\mathbf{y}_i = \mathbf{y}_i^1 - \mathbf{y}_i^2.$$

More generally, if the opponent is assumed to be able to collect a large number of randomly distributed plaintexts and the corresponding ciphertexts. He may be able to derive MN independent known plaintexts $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_i, \cdots, \mathbf{x}_{MN}$, and to recover the equivalent key $\mathbf{T}\Phi$ by

$$\mathbf{T}\Phi = \mathbf{X}^{-1}\mathbf{Y}$$

where $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_i, \cdots, \mathbf{x}_{MN}]$ are MN known-plaintexts and $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_i, \cdots, \mathbf{y}_{MN}]$ are the corresponding ciphertexts. Referring to the coupon collector problem [34], there exist MN independent plaintexts in the collection of $O(MN \times \log MN)$ plaintexts with large probability, i.e., the data complexity of this known-plaintext attack is $O(MN \times \log MN)$.

3.5. Ciphertext-Only Attack

Referring to the achievements in the previous subsection, one can conclude that the combined cryptosystems can be regarded as novel CS encodes with the measurement matrices consisting of that of the original CS and the random phase keys. The resistance of the cascaded system with either C-D or D-C architecture against ciphertext-only attack equivalents to that of the standard CS process, i.e., the cascaded systems do not achieve perfect secrecy, whereas possess computation notion of secrecy [23].

3.6. Simulation Results

Computer simulations have been carried out to validate the above cryptanalysis. The employed measurement matrix of CS is Gaussian random matrix, and the phase masks of DRPE are generated with *rand* function of Matlab. It should be emphasized that, the proposed cryptanalysis is effective for the general ciphers combining DRPE with CS, no matter what the measurement matrix is or the implementation order of the two procedures. The result presented here is just a demonstration of the effectiveness, it straightforward to extend the cryptanalysis to various encryption scenarios[1]. The operation steps of the C-D type encryption is therefore firstly compressively sampling the plaintext and then encrypting the measurements using DRPE, whereas the implementations of D-C scheme is ciphering the plaintxt using DRPE and subsequently compressed sampling the DRPE ciphertext. The sample rate of CS is adopted as 0.5 for demonstration. The verification steps are: 1) encrypting the plaintext using both the C-D and D-C systems; 2) launching the chosen-plaintext attack to retrieve the equivalent secret keys ($\mathbf{T}\Phi$ or $\Phi\mathbf{T}$); 3) decrypting the plaintext according to Eqs. (17) and (18). Two plaintexts with size of 128×128 are introduced, the first one is the peppers image, and the other one is a CT image of abdomen.

[1]The source codes are openly accessible at https://sites.google.com/site/leoyuzhang/.

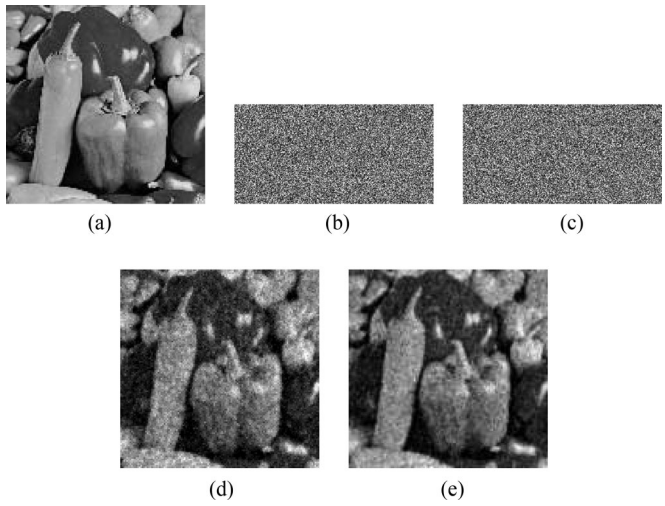


Fig. 4. The encryption results of C-D and D-C cryptosystems: (a) plaintext peppers, (b) amplitude of the ciphertext using C-D scheme, (c) amplitude of the ciphertext of D-C system, (d) recovery of the C-D scheme, (e) recovery of the D-C scheme.

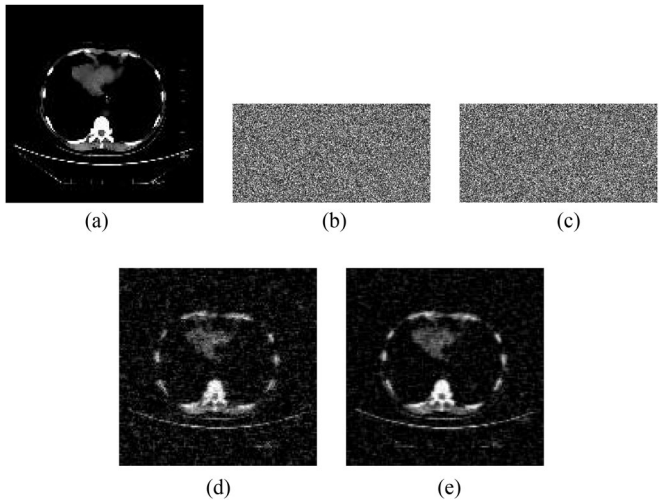


Fig. 5. The encryption results of C-D and D-C cryptosystems: (a) plaintext CT-Abdomen, (b) amplitude of the ciphertext using C-D scheme, (c) amplitude of the ciphertext of D-C system, (d) recovery of the C-D scheme, (e) recovery of the D-C scheme.

The plaintext peppers is shown in Fig. 4(a), and the amplitudes of the ciphertexts of C-D and D-C cryptosystems are demonstrated in Fig. 4(b) and (c), respectively. The retrieved equivalent encryption matrices under the chosen-plaintext attack, i.e., $\mathbf{T}\Phi$ and $\Phi\mathbf{T}$, are partly given in Eqs. (20) and (21). Obviously, one cannot derive the precise knowledge of Φ and $\mathbf{T}$ from their product. Yet, it is also not necessary to do this, as the proved RIP performance of the matrices reveals that the recovery of the plaintext can be relaxed to a single-step ℓ_1 optimization. Specially speaking, the reconstruction of Fig. 4(b) and (c) is performed with the help of these retrieved keys and Eqs. (17) and (18). The recovered images of C-D and D-C cryptosystems are demonstrated in Fig. 4(d) and (e) with the PSNRs are 20.39 dB and 21.23 dB, respectively. Another set of simulation results is demonstrated in Fig. 5, with PSNRs are 20.02 dB and 21.05 dB for the retrieved images of C-D and D-C schemes, respectively. From the above tests, the effectiveness of the proposed cryptanlaysis

has therefore been well validated.

$$Key_{C-D} = \mathbf{T}\Phi = \begin{bmatrix} -1.256 + 0.321i & 0.834 + 0.986i & \cdots & 0.522 + 0.337i \\ -0.049 - 0.121i & -0.302 - 0.175i & \cdots & -0.409 + 0.049i \\ \vdots & \vdots & \ddots & \vdots \\ 0.511 - 0.081i & 0.048 - 1.099i & \cdots & 0.601 - 0.117i \end{bmatrix}. \quad (20)$$

$$Key_{D-C} = \Phi\mathbf{T} = \begin{bmatrix} 0.206 + 0.291i & -0.588 + 0.866i & \cdots & 0.897 + 0.728i \\ -1.451 - 0.089i & 0.136 - 1.040i & \cdots & -0.503 + 0.129i \\ \vdots & \vdots & \ddots & \vdots \\ 0.071 + 0.674i & -0.621 + 1.034i & \cdots & -0.639 + 0.141i \end{bmatrix}. \quad (21)$$

4. Conclusion

In this paper, we present the security evaluation of optical ciphers combining CS with DRPE together. Cryptanalyses of both the alternative combination pattens, i.e., C-D or D-C, have been given out. It is shown that such cryptosystems can be ultimately summed up as a linear decoder, whose equivalent key matrix can be retrieved through plaintext attack. With the recovery of the equivalent matrix, only a single-step optimization is sufficient to break the whole system. We believe that our work can help researchers in this area to design secure and efficient cryptosystems with CS and DRPE.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and fourier planerandom encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[2] 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.*, vol. 30, no. 13, pp. 1644–1646, 2005.

[3] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.*, vol. 31, no. 8, pp. 1044–1046, 2006.

[4] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Exp.*, vol. 15, no. 16, pp. 10 253–10 265, 2007.

[5] Z. Liu, C. Shen, J. Tan, and S. Liu, "A recovery method of double random phase encoding system with a parallel phase retrieval," *IEEE Photon. J.*, vol. 8, no. 1, Feb. 2016, Art. no. 7801807.

[6] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, 2000.

[7] N. Singh and A. Sinha, "Gyrator transform-based optical image encryption, using chaos," *Opt. Lasers Eng.*, vol. 47, no. 5, pp. 539–546, 2009.

[8] G. Situ and J. Zhang, "Double random-phase encoding in the fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, 2004.

[9] X. C. Cheng *et al.*, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett.*, vol. 33, no. 14, pp. 1575–1577, 2008.

[10] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated fourier transforms," *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, 2010.

[11] A. Elshamy *et al.*, "Optical image encryption based on chaotic baker map and double random phase encoding," *IEEE J. Lightw. Technol.*, vol. 31, no. 15, pp. 2533–2539, Aug. 2013.

[12] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic baker map and double random phase encoding," *J. Opt.*, vol. 16, no. 12, 2014, Art. no. 125403.

[13] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.*, vol. 36, no. 1, pp. 22–24, 2011.

[14] C. Shen, J. Tan, C. Wei, and Z. Liu, "Coherent diffraction imaging by moving a lens," *Opt. Exp.*, vol. 24, no. 15, pp. 16520–16529, 2016.

[15] W. Chen and X. Chen, "Double random phase encoding using phase reservation and compression," *J. Opt.*, vol. 16, no. 2, 2014, Art. no. 025402.

[16] X. Wang, W. Chen, and X. Chen, "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes," *Opt. Exp.*, vol. 23, no. 5, pp. 6239–6253, 2015.

[17] W. Chen, X. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," *IEEE Photon. J.*, vol. 5, no. 2, Apr. 2013, Art. no. 6900113.

[18] X. Wang, W. Chen, and X. Chen, "Optical encryption and authentication based on phase retrieval and sparsity constraints," *IEEE Photon. J.*, vol. 7, no. 2, 2015, Art. no. 7800310.

[19] E. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[20] D. Donoho, "Compressed sensing," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[21] E. Candes and M. Wakin, "An introduction to compressive sampling," *IEEE Trans. Signal Process.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.
[22] E. Candes and T. Tao, "Near-optimal signal recovery from random projections: Universal encoding strategies?" *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.
[23] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 2008 46th Annu. Allerton Conf. Commun., Control, Comput.*, 2008, pp. 813–817.
[24] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2182–2195, Oct. 2015.
[25] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, "Bi-level protected compressive sampling," *IEEE Trans. Multimedia*, vol. 18, no. 9, pp. 1720–1732, Sep. 2016.
[26] B. Deepan, C. Quan, Y. Wang, and C. J. Tay, "Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique," *Appl. Opt.*, vol. 53, no. 20, pp. 4539–4547, 2014.
[27] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik—Int. J. Light Electron Opt.*, vol. 124, no. 16, pp. 2514–2518, 2013.
[28] N. Rawat, B. Kim, I. Muniraj, G. Situ, and B.-G. Lee, "Compressive sensing based robust multispectral double-image encryption," *Appl. Opt.*, vol. 54, no. 7, pp. 1782–1793, 2015.
[29] N. Rawat, I.-C. Hwang, Y. Shi, and B.-G. Lee, "Optical image encryption via photon-counting imaging and compressive sensing based ptychography," *J. Opt.*, vol. 17, no. 6, 2015, Art. no. 065704.
[30] T. Do, L. Gan, N. Nguyen, and T. Tran, "Fast and efficient compressive sensing using structurally random matrices," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 139–154, Jan. 2012.
[31] K. R. Rao, D. N. Kim, and J. J. Hwang, *Fast Fourier Transform-Algorithms and Applications*. New York, NY, USA: Springer, 2011.
[32] J. W. Brewer, "A note on kronecker matrix products and matrix equation systems," *SIAM J. Appl. Math.*, vol. 17, no. 3, pp. 603–606, 1969.
[33] H. Fang, S. Vorobyov, H. Jiang, and O. Taheri, "Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals," *IEEE Trans. Signal Process.*, vol. 62, no. 1, pp. 196–210, Jan. 2014.
[34] D. Brian, "Siobhan's problem: The coupon collector revisited," *Amer. Statistician*, vol. 45, no. 1, pp. 76–82, 1991.