Cryptanalysis of optical ciphers integrating double random phase encoding with permutation

CHEN, JUNXIN; BAO, NAN; LI, JINCHANG; ZHU, ZHI-LIANG; ZHANG, LEO YU

Published in:
IEEE Access

Online published: 09/08/2017

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

License:
Unspecified

Publication record in CityU Scholars:
Go to record

Published version (DOI):
10.1109/ACCESS.2017.2735420

Publication details:

Citing this paper
Please note that where the full-text provided on CityU Scholars is the Post-print version (also known as Accepted Author Manuscript, Peer-reviewed or Author Final version), it may differ from the Final Published version. When citing, ensure that you check and use the publisher's definitive version for pagination and other details.

General rights
Copyright for the publications made accessible via the CityU Scholars portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights. Users may not further distribute the material or use it for any profit-making activity or commercial gain.

Publisher permission
Permission for previously published items are in accordance with publisher's copyright policies sourced from the SHERPA RoMEO database. Links to full text versions (either Published or Post-print) are only available if corresponding publishers allow open access.

Take down policy
Contact lbscholars@cityu.edu.hk if you believe that this document breaches copyright and provide us with details. We will remove access to the work immediately and investigate your claim.

Download date: 04/06/2022
Cryptanalysis of Optical Ciphers Integrating Double Random Phase Encoding With Permutation

JUNXIN CHEN¹, NAN BAO¹, JINCHANG LI¹, ZHI-LIANG ZHU², (Member, IEEE), AND LEO YU ZHANG³,⁴, (Member, IEEE)

¹Sino-Dutch Biomedical and Information Engineering School, Northeastern University, Shenyang 110169, China
²Software College, Northeastern University, Shenyang 110169, China
³School of Information Technology, Jinan University, Guangzhou 510632, China
⁴Department of Electronic Engineering, City University of Hong Kong, Hong Kong

Corresponding author: Junxin Chen (chenjx@bmie.neu.edu.cn) and Leo Yu Zhang (leocityu@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61374178 and in part by the Fundamental Research Funds for the Central Universities under Grant N162410002-4.

ABSTRACT This paper presents the cryptanalysis of optical ciphers combining double random phase encoding with permutation techniques, and shows its vulnerability against plaintext attack regardless of the implementation order of the two procedures. The equivalent secret keys of both the combination fashions can be retrieved, instead of the recovery of random phase masks and permutation matrix. Numerical simulations are also given for validation.

INDEX TERMS Double random phase encoding, optical ciphers, image permutation, cryptanalysis.

I. INTRODUCTION

In the past decades, the inherent parallelism superiority has promoted the developments of optical information processing techniques. Among them, double random phase encoding (DRPE), which is used to protect confidentiality of images by transforming them into stationary white noises, has paved the way for numerous types of optical security schemes since its appearance in [1]. Originating from the intrinsic linearity feature, DRPE is demonstrated to be vulnerable against various attacks, such as chosen-ciphertext attack [2], known-plaintext attack [3], chosen-plaintext attack [4], and some of its enhancements have also been broken [5]–[7].

For security improvements, permutation techniques, such as Jigsaw transform [8], Chirikov standard map [9], and chaotic Baker map [10], [11] have been introduced to combine with DRPE to build secure cascaded cryptosystems. There are two integration fashions. The first type uses a preprocessing scrambling before DRPE (permutation-then-DRPE, abbreviated as PD), a typical scheme is proposed in [10]. The latter pattern is to adopt a rear-mounted permutation procedure (DRPE-then-permutation, abbreviated as DP), a representative design can be found in [11]. Cryptanalysis of the first type cascaded system has been investigated in [11], [12], whereas the vulnerability of DP scheme has not been proposed. In this work, we will give a general cryptanalysis of the optical ciphers combining DRPE with permutation technique, no matter what’s the order of the two procedures.

This study differs from the previous achievement [12], which only presents the chosen-plaintext attack for PD scheme, in that we demonstrate a generalized cryptanalysis of both the PD and DP cryptosystems and give an effective plaintext attack for both types of the combined systems. In other words, this work can be viewed as an extension of [12], not only in theoretical analysis but also in the universality for breaking the cascaded systems. The proposed achievement is a generalized cryptanalysis of the encryption systems combining DRPE with permutation, no matter how complex the permutation technique is and what the implementation order of the two procedures. Our contributions can be summarized as following: 1) the equivalent form of DRPE is deduced out, the linearity and vulnerability of DRPE is intuitively exposed; 2) cryptanalysis shows that both the combined systems can be viewed as linear encoding schemes, whose equivalent encryption matrices are also given; 3) the unitary of the equivalent encryption matrices are proved, which relax the decryption/breaking of the cryptosystems to a matrix conjunction-then-multiplication operation rather
than the recovery of the permutation matrix as well as the random phase masks. The proposed achievements reveal that the security of such combined systems cannot be improved by developing more complex permutation approaches, or adjusting the implementation order of DRPE and permutation procedures.

The remainder of this paper is organized as follows. The combined cryptosystems and theoretical preliminaries are given in section II, while the cryptanalysis is described in detail in section III. Experimental results is presented in section IV. Finally, conclusions will be drawn in the last section.

II. PRELIMINARIES

Let us start with the baisc principle of DRPE. It is based on 4f optical system to encrypt the plaintext into stationary white noise. As illustrated in Fig. 1, the primary image X is immediately followed by a random phase mask R1, they are placed in the object plane of the first lens. Then in the focal plane of this lens, the Fourier transform (FT) of the product $X \cdot R1$, is obtained. This product is subsequently multiplied by the second random phase mask R2, and then be converted to spatial domain by the second lens. The encryption and decryption processes can be respectively written as Eqs. (1) and (2), where $\ast$ represents the conjugation, $F$ denotes the two-dimensional Discrete Fourier Transform (2D DFT) and $F^{-1}$ is the two-dimensional inverse Discrete Fourier transform (2D IDFT). The random phase masks R1 and R2 serve as the secret key.

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

$$X = F^{-1}(F(C) \cdot R2^\ast) \cdot R1^\ast. \quad (2)$$

Without loss of generality, P is denoted as the scrambling transformation. Figure 2(a) sums up the encryption operations of PD scheme, while Fig. 2(b) demonstrates that of the DP cryptosystem. Taking Eq. (1) into consideration, we can subsequently obtain the outputs of PD and DP, as shown in Eqs. (3) and (4), respectively.

$$C_{PD} = F^{-1}(R2 \cdot F(P(X) \cdot R1)). \quad (3)$$

$$C_{DP} = P(F^{-1}(R2 \cdot F(X \cdot R1))). \quad (4)$$

Theoretical preliminaries regarding Fourier transform and Kronecker product are required for the cryptanalysis. The descriptions or proofs of the subsequent theoretical preliminaries are either straight-forward or can be found in [13], [14], and hence not presented here.

**Definition 1:** The $F_N$ is defined as the Fourier matrix which can convert the DFT of a length−N signal through matrix multiplication, i.e., $F_N(x) = F_{Nx}$. The formula of $F_N$ is described in Eq. (5), where $w = e^{-2\pi i/N}$ is a primitive Nth root of unity.

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & w^3 & \cdots & w^{N-1} \\ 1 & w^2 & w^4 & w^6 & \cdots & w^{2(N-1)} \\ 1 & w^3 & w^6 & w^9 & \cdots & w^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & w^{3(N-1)} & \cdots & w^{(N-1)(N-1)} \end{bmatrix}. \quad (5)$$

**Property 1:** Both of the Fourier matrix $F_N$ and its conjugate transpose $F_N^H$ are symmetric and unitary, i.e., Eqs. (5) and (6) always hold.

$$F_N = F_N^T. \quad (5)$$

$$F_N^{-1} = F_N^H = F_N^{HT}. \quad (6)$$

**Theorem 1:** With the definition of Fourier matrix, the 2D $M \times N$ DFT and IDFT can be respectively described...
as Eqs. (7) and (8).
\[
\mathcal{F}(P_{M\times N}) = F_M P_{M\times N} F_N^H. \\
\mathcal{F}^{-1}(P_{M\times N}) = F_M^H P_{M\times N} F_N.
\]  

Property 2: Denote X and R be M × N matrices, and ‘vec’ command as the vectorization operation to reshape a matrix to a vector by stacking its columns, it is found that Eq. (9) always holds, where diag(vec(R)) is the diagonal matrix with entries are the sequential components of vec(R).
\[
vec(X \cdot R) = vec(R \cdot X) = \text{diag}(vec(R))vec(X).
\]  

Definition 2: If A is an M × N matrix and B is a P × Q matrix, then the Kronecker product A ⊗ B is an MP × NQ block matrix:
\[
A \otimes B = \begin{bmatrix}
a_{11}B & \cdots & a_{1N}B \\
\vdots & \ddots & \vdots \\
a_{M1}B & \cdots & a_{MN}B
\end{bmatrix}.
\]  

Property 3: (A ⊗ B)^H = A^H ⊗ B^H.
Property 4: (A ⊗ B)(C ⊗ D) = (AC) ⊗ (BD).

Theorem 2: Assume that C = AXB, it has vec(C) = vec(AXB) = (B^T ⊗ A)vec(X).

III. CRYPTANALYSIS

The equivalent of DRPE has to be deduced firstly. In the following, we consider DRPE from the vector point of view. The lowercase letter x is reserved as the corresponding vector of the matrix X by stacking its columns. Taking Eqs. (7) and (8) into Eq. (1), we obtain
\[
C = F_M^H (R \cdot F_M (X \cdot R1) F_N) F_N^H.
\]

Considering Theorem 2, we can get
\[
vec(C) = vec(F_M^H (R \cdot F_M (X \cdot R1) F_N) F_N^H) \\
= (F_M^H \otimes F_N^H)vec(R \cdot F_M (X \cdot R1) F_N).
\]

And then, taking Properties 1 and 2 into consideration,
\[
vec(C) = (F_M^H \otimes F_N^H)vec(R \cdot F_M (X \cdot R1) F_N) \\
= (F_M^H \otimes F_N^H) diag(vec(R))(F_M \otimes F_N)(X \cdot R1).
\]

Employing Theorems 1 and 2 and Properties 2 and 3 further, we can obtain
\[
vec(C) \times diag(vec(R)) = (F_M \otimes F_M)diag(vec(R))(F_M \otimes F_N)(X \cdot R1).
\]

Here, the equivalent of DRPE is obtained, as demonstrated in Eq. (11), where \(\mathbb{F}\) is the Kronecker product of \(F_N\) and \(F_M\). \(\mathbb{R} = \text{diag}(\text{vec}(R1)), \mathbb{R}2 = \text{diag}(\text{vec}(R2))\), and T is adopted as the product of \(\mathbb{F}^H \mathbb{R}2 \mathbb{F}1\), respectively. They are all with size \(MN \times MN\), whereas the size of the input X is \(M \times N\) and will be vectorized to x with size \(MN \times 1\).
\[
c = vec(C) = \mathbb{F}^H \mathbb{R}2 \mathbb{F}1 x = Tx.
\]

Generally, the random scrambling operation is given as a permutation matrix whose size is identical with the primary image, and its particle is a 2D pixel coordinate denotes the scrambled position in the permuted image, as the preferred case in [11], [15], and [16]. On the contrary, the permutation operation is treated from the vector point of view in this work. In this circumstance, the permutation is implemented to a length-MN vector x rather than M × N matrix X. The permutation matrix is regarded as a uniform random MN × MN permutation matrix, with ‘1’ occurring once and only once in each row and column and all other entries are ‘0’. It can be regarded as the random arrangement of the rows/columns of MN × MN identity matrix. Referring to the deduction above, we can draw the ciphertexts of PD and DP schemes in Eqs. (12) and (13), respectively. Accordingly, the products \(TP\) and \(PT\) can be respectively regarded as the equivalent keys of the PD and DP encryption schemes.
\[
c_{PD} = vec(C_{PD}) = \mathbb{F}^H \mathbb{R}2 \mathbb{F}1 x = TPx
\]
\[
c_{DP} = vec(C_{DP}) = \mathbb{F}^H \mathbb{R}2 \mathbb{F}1 x = PTx
\]

Here, one can draw the conclusion that MN pairs of chosen-plaintexts are sufficient to retrieve the equivalent secret keys, i.e., \(TP\) and \(PT\), no matter how complex the permutation is and what the implementation sequence of the two procedures. In practice, the attack can be launched using MN independent plaintexts, i.e., \(x_i = \{x_{i1}, x_{i2}, \ldots , x_{im}, \ldots , x_{iMN}\}\). For example, \(x_i\) can be one column of the MN × MN identity matrix, and its ciphertext \(y_i\) is therefore the corresponding column of the equivalent keys. After the extraction of the equivalent matrix key \(TP\) or \(PT\), their inverse could be used for recovering any ciphertexts which are produced with the same secret key.

It can be further proved that both \(TP\) and \(PT\) are unitary matrices, so that the expensive matrix inversion reduces to the simple conjugate transpose operation.

The unitarity of T is proved at first. As described before, \(T = \mathbb{F}^H \mathbb{R}2 \mathbb{F}1\), where \(\mathbb{F}\) is the Kronecker product of \(F_N\) and \(F_M\). Based on Properties 3 and 4, we obtain
\[
\mathbb{F}^H = (F_N \otimes F_M)(F_N \otimes F_M)^H = (F_N \otimes F_M)(F_N^H \otimes F_M^H) = (F_N F_N^H) \otimes (F_M F_M^H) = I \otimes I = I.
\]

That means \(\mathbb{F}\) is unitary. Considering \(\mathbb{R}1\) and \(\mathbb{R}2\) are built by phase-only matrices, and hence are unitary, we can consequently obtain
\[
TT^H = (\mathbb{F}^H \mathbb{R}2 \mathbb{F}1)(\mathbb{F}^H \mathbb{R}2 \mathbb{F}1)^H = I.
\]

Therefore, T is proved as a unitary matrix. Moreover, it is always true that further permuting a shuffled sequence \(Px\)
with $P^T$ will re-produce the original sequence $x$. In light of these observations, it is readily to conclude that $TP$ and $PT$ are both unitary.

With the extraction of the equivalent keys, i.e., one has obtained the product of $TP$ or $PT$ by plaintext attack, only a conjunction-then-multiplication operation is sufficient to recover the plaintext. It is un-necessary, if it is not unable, to retrieve the permutation matrix $P$ and the DRPE equivalent key $T$, respectively. The recovery of the plaintext can be straightforward implemented, as illustrated in Eqs. (14) and (15), for PD and DP schemes, respectively.

$$x = \text{vec}(X) = (TP)^{-1}c_{DP} = (TP)^Hc_{PD} \quad (14)$$
 $$x = \text{vec}(X) = (PT)^{-1}c_{PD} = (PT)^Hc_{DP} \quad (15)$$

We can come to the conclusion that, both of the PD and DP encryption schemes are vulnerable against chosen-plaintext attack, and the number of the required plaintexts is $MN$. Besides, referring to the coupon collector problem [17], 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 $O(MN \times \log MN)$.

**IV. NUMERICAL SIMULATION**

To validate the above cryptanalysis, numbers of numerical simulations have been carried out to crack the typical PD scheme proposed by Elshamy [10] and the representative DP cryptosystem in [11]. The same secret key, i.e., identical phase masks and Baker map parameters are adopted in both systems. The encryption algorithms and cryptanalyzing operations are implemented on Matlab R2010a platform, using a personal computer with an Intel(R) Core(TM)i5 CPU (3.2GHZ), 16GB memory and 1TB hard-disk capacity. The result presented here is just a demonstration of the effectiveness, it is straightforward to extend the cryptanalysis to various encryption scenarios with the source codes openly accessible at https://sites.google.com/site/leoyuzhang/.

The gray-scale peppers image with size of $256 \times 256$ is employed for validation, shown in Figs. 3(a) and 4(a). The effectiveness of the proposed cryptanalysis for PD scheme [10] is demonstrated in Fig. 3, where Figs. 3(b) and 3(c) are the amplitude and phase of the ciphertext, respectively.

As can be observed, the ciphertexts are noisy-like and does not release any useful information of the plaintext. We then lanuch the chosen-plaintext attack to extract the equivalent encryption matrix, partly demonstrated in Eq. (16), as shown at the bottom of this page. As analyzed above, this encryption matrix is a product of the permutation matrix and the random phase masks, and it is not necessary to do this. The proved unitarity of the encryption matrix relaxes the decryption process to a matrix conjunction-then-multiplication operation, as shown in Eqs. (14) and (15), for PD and DP schemes, respectively. With this method, the plaintext is subsequently correctly recovered, as shown in Fig. 3(d).

The simulation results when cryptanalyzing DP scheme are given in Fig. 4, and Eq. (17), as shown at the bottom of this page, is the retrieved equivalent matrix using the proposed attack. It is obvious that the equivalent secret keys are different even though using identical phase masks and permutation matrix, i.e., different implementation orders brings distinct ciphertexts.

The recovered image with the retrieved keys is shown in Fig. 4(d). Numerical analysis proves that both the
The recovered images are consistent with the plaintext, and therefore validate the effectiveness of the proposed attack.

V. CONCLUSIONS

In summary, we have demonstrated that encryption schemes combining DRPE with permutation technique are vulnerable against plaintext attack regardless of the implementation order. From the vector point of view, both of the two techniques can be regarded as linear transforms. They cannot enhance the security for each other, the vulnerability originates from the intrinsic linear property.

REFERENCES


ZHI-LIANG ZHU received the M.S. degree in computer applications and the Ph.D. degree in computer science from Northeastern University, China. He is currently a Fellow with the China Institute of Communications. He has authored and co-authored over 130 international journal papers and 100 conference papers. His main research interests include information integration, complexity software systems, network coding and communication security, chaos-based digital communications, applications of complex network theories, and cryptography. He is also a recipient of nine academic awards at national, ministerial, and provincial levels. He currently serves as Co-Chair of the 9th International Workshop on Chaos-Fractals Theories and Applications. He is a Senior Member with the Chinese Institute of Electronics and the Teaching Guiding Committee for Software Engineering under the Ministry of Education.

LEO YU ZHANG (S’14–M’17) received the bachelor’s and master’s degrees in computational mathematics from Xiangtan University, Xiangtan, China, in 2009 and 2012, respectively, and the Ph.D. degree from the City University of Hong Kong, Hong Kong, in 2016. He is a Post-Doctoral Fellow with the College of Information Science and Technology, Jinan University, Guangzhou, China. He held various research positions with the City University of Hong Kong, the University of Macau, Macau, China, the University of Ferrara, Ferrara, Italy, and the University of Bologna, Bologna, Italy. His current research interests include cloud security, multimedia security, and compressed sensing.