Universal and special keys based on phase-truncated Fourier transform

Wan Qin
Xiang Peng
Xiangfeng Meng
Bruce Gao
Universal and special keys based on phase-truncated Fourier transform

Wan Qin,a,b Xiang Peng,a Xiangfeng Meng,c and Bruce Gaoa

aShenzhen University, College of Optoelectronics Engineering, Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education, Shenzhen 518060, China
bClemson University, Department of Bioengineering, Clemson, South Carolina 29634
cShandong University, School of Information Science and Engineering, Jinan 250100, China
E-mail: tylgqinwan@163.com

Abstract. We propose a novel optical asymmetric cryptosystem based on a phase-truncated Fourier transform. Two decryption keys independent of each other are generated. They are referred to as universal key and special key, respectively. Each of them can be used for decryption independently in absence of the other. The universal key is applicable to decrypt any ciphertext encoded by the same encryption key, but with poor legibility. On the contrary, the special key is adequate for legible decryption, but only valid for one ciphertext corresponding to the specified plaintext. A set of simulation results show the interesting performance of two types of decryption keys.

Subject terms: phase-truncated Fourier transform; optical encoding; asymmetric encryption.

During the past decade, a lot of effort has been made to develop the techniques of optical cryptography owing to the inherent nature of parallel and multidimensional capability of optical signal processing.1–3 Most of those optical cryptosystems employ random phase masks (RPMs) as secret keys due to the advantage of huge key space. They always contribute to resistance of an encryption scheme against brute force attacks. However, RPMs are not sufficiently sensitive as expected. This may result in another security worry. It has been recently demonstrated that the double random phase encoding scheme is vulnerable to known-plaintext attacks.4–6 With phase retrieval techniques, an attacker can easily find the estimates of RPM keys, with which the attacker can recover the plaintext from the corresponding ciphertext. Nevertheless, using phase retrieval strategy to access estimates of RPM keys is only available for linear systems. From another perspective, if employing an appropriate nonlinear transform for encryption, we find out that the insensitivity of RPM will not only avoid suffering a potential crack, but also may allow a cryptosystem possessing other unique features, as introduced later.

From the cryptography point of view, a symmetric cryptosystem would suffer from several problems in practical use, in particular, under the network environment such as key distribution and management.7,8 Asymmetric scheme is the solution. In this paper, we design a novel asymmetric optical encryption system, in which two different types of decryption keys are particularly involved, named universal key $K_u$, and special key $K_s$, respectively. The decryption keys differ from the encryption key. Each decryption key has its own function and applicable region in the process of decryption. One universal key corresponds to one encryption key ($K_e$). $K_u$ can be used to decrypt any ciphertext encoded by $K_e$, but with poor legibility. On the contrary, $K_s$ is adequate for legible decryption but only valid for one ciphertext corresponding to the specified plaintext.

Now let us discuss the detail about this asymmetric cryptosystem. Phase-truncated Fourier transform (PTFT), which is proposed in our earlier work for the construction of optical asymmetric cryptosystem,9 is used again here to build a multifunctional scheme. PTFT is a process of Fourier transform with an operation of phase truncation, which means only the amplitude (modular part) of Fourier spectrum is retained, while the phase part of the spectrum is truncated. For the sake of simplicity, one-dimensional notation is used to illustrate this concept. Let $f(x)$ denote the image to be encoded, $\text{FT}(\cdot)$ the operator of Fourier transform, $\text{PT}(\cdot)$ the operator of phase truncation, and $\text{PR}(\cdot)$ the operator of phase reservation. Given a Fourier transformation $F(u) = \text{FT}[f(x)] = [F(u)] \exp[i2\pi\varphi(u)]$, the phase truncation and the phase reservation can be respectively expressed as follows:

$$\text{PT}[F(u)] = |F(u)|,$$  \hspace{1cm} (1)

$$\text{PR}[F(u)] = \exp[i2\pi\varphi(u)].$$ \hspace{1cm} (2)

By implementing the phase-truncated Fourier transform, one can encrypt a plaintext into a noise-like cipher. The encryption process is illustrated in Fig. 1(a). Let $P_1$ denote an image plaintext and $C_1$ the corresponding ciphertext. The encoded image $C_1$ can be obtained by the following equation:

$$C_1(u) = \text{PT}[\text{FT}[P_1(x) \cdot K_e(x)]] .$$ \hspace{1cm} (3)

Although simple, the encryption should hold a higher security level than the classic double random phase encoding scheme, because the operation of phase truncation is nonlinear. From this point of view, the technique of phase retrieval will be invalid for estimating the phase key. Moreover, the most noticeable point of this optical cryptosystem does not lay in the improvement of security strength but in the existence of a universal key and special key. Figure 1(b) depicts how to generate a universal key. Performing a Fourier transformation on the encryption key and retaining the phase part, we obtain the universal key as follows:

$$K_u(u) = \text{PR}[\text{FT}[K_e(x)]] .$$ \hspace{1cm} (4)

The special key is recorded in the process of encryption [as shown in Fig. 1(a)] by the following equation:

$$K_s(u) = \text{PR}[\text{FT}[P_1(x) \cdot K_e(x)]] .$$ \hspace{1cm} (5)

It is interesting to note that both $K_s$ and $K_u$ can be used for the purpose of decryption, as shown in Fig. 1(c). When employing $K_s$, the decryption is just a reverse operation of the encryption. Under an ideal circumstance, the decryption is lossless because the truncated information is compensated.

0091-3286/2011/$25.00 © 2011 SPIE
Fig. 1 Flowchart of (a) encryption process with PTFT, (b) generation of universal key, and (c) decryption process.

Mathematically, it can be written as

\[ P_1(x) = PT \{ IFT \{ C_1(u) \cdot K_e(u) \} \} \quad (6) \]

where IFT(·) denotes the inverse Fourier transform. However, \( K_e \) is only applicable to decrypt \( C_1 \) because \( K_e \) is generated from \( P_1 \), whereas \( K_s \) is applicable to decrypt any ciphertext encoded with \( K_e \). If substituting \( K_s \) for \( K_e \) in Eq. (6), one can still retrieve \( P_1 \) except for being blurred as

\[ P'_1(x) = PT \{ IFT \{ C_1(u) \cdot K_s(u) \} \} \]
\[ = PT \{ IFT \{ FT \{ P_1(x) \cdot K_e(x) \} \cdot B(u) \} \} \quad (7) \]

where \( B(u) \) is a blurring function given by

\[ B(u) = \frac{K_s(u)}{K_e(u)} = \frac{PR \{ FT \{ K_e(x) \} \}}{PR \{ FT \{ K_e(x) \} \odot FT \{ K_e(x) \} \}} \]

where \( \odot \) means convolution. If the plain image has only low frequency content, \( FT \{ P_1(x) \} \) will be narrow and \( B(u) \) will be close to 1, leading to a good decryption. Therefore, the blurring degree of the decryption result depends on the frequency content of the plaintext. It should be noted that the proposed encryption strategy is only suitable for phase-only keys and real-value plaintexts. If either of them is complex-valued, the decryption function [Eq. (6)] will be invalid.

Now we perform a proof-of-concept study with the aid of computer simulation in the environment of MATLAB. Consider images \( P_1 \) (Lena, 256×256 pixels) and \( P_2 \) (Baboon, 256×256 pixels) as two plaintexts. The ciphertexts, obtained with PTFT strategy, are two noise-like images, \( C_1 \) and \( C_2 \) (they are not shown here for saving space). The encryption key \( K_e \) is a random phase mask with the same size as the plaintexts. By using Eq. (4), we can obtain the universal decryption key \( K_u \). Two special decryption keys, \( K_{s1} \) and \( K_{s2} \), corresponding to plaintexts \( P_1 \) and \( P_2 \), respectively, are generated in each encryption process, according to Eq. (5). Now let us verify the effectiveness of decryption using the universal key and the special keys, respectively. When the special key \( K_{s1} \) corresponding to the first plaintext \( P_1 \) was used to decrypt \( C_1 \), the Lena image can be clearly recovered, as shown in Fig. 2(a), whereas when \( K_{s1} \) was used to decrypt \( C_2 \), Baboon cannot be retrieved, as shown in Fig. 2(f). Similarly, the special key \( K_{s2} \) corresponding to plaintexts \( P_2 \) also can only be used to effectively decode \( C_2 \) [see Fig. 2(d)], and cannot be used to recover Lena [see Fig. 2(c)]. These results proved that special keys are only legal for decryptations of the specified ciphertexts. With the right special key, it is lossless to decode the specified cipher but incapable of decoding others. In another case, when the universal key is used in the process of decryptions, both \( P_1 \) and \( P_2 \) can be approximately retrieved although being corrupted by noise, as shown in Figs. 2(b) and 2(e).

The computer simulation results demonstrate that the proposed optical cryptosystem can possess two independent decryption keys. This is quite a different case from that in traditional cryptography. This unique property of the proposed approach may allow the PTFT-based scheme to be used for envisaged application cases. As an example, case 1 would be to secure communications of simple messages (such as binary letters) between the members of a large group. In this case, the decryption effect of a universal key is adequate for the identification of plain messages. Thus, the PTFT scheme could serve as an ordinary asymmetric cryptosystem, regardless of the existence of special keys. As another example, case 2 would be high-security-level communication of delicate messages between two nodes in a network. In this case, the universal key would be irrelevant for the process of decryption, whereas the special key could be used to retrieve the messages precisely. Meanwhile, the security level could be guaranteed in virtue of the one-time pad manner. Some other possible cases may include setting up the security levels for different users, identification and authentication with different security levels, etc.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 60775021 and 60777008), IIFSDU (Grant No. 2010TB019), NIH (SC...
References