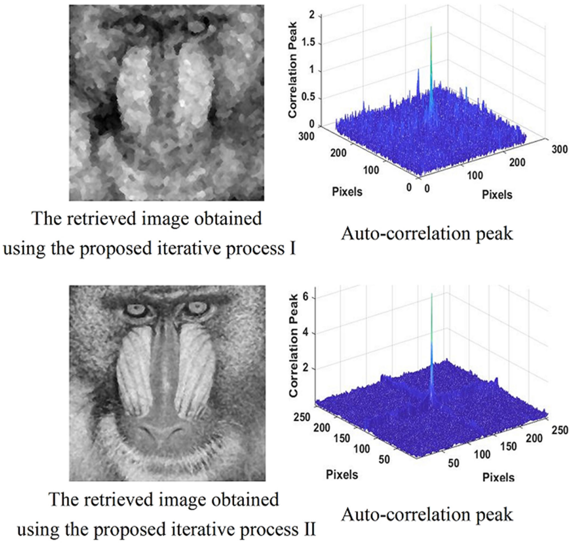
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Security Analysis on an Optical Encryption and Authentication Scheme Based on Phase-Truncation and Phase-Retrieval Algorithm

Volume 11, Number 5, October 2019

Yi Xiong
Ravi Kumar
Chenggen Quan



The retrieved image obtained using the proposed iterative process I

Auto-correlation peak

The retrieved image obtained using the proposed iterative process II

Auto-correlation peak

DOI: 10.1109/JPHOT.2019.2936236

Security Analysis on an Optical Encryption and Authentication Scheme Based on Phase-Truncation and Phase-Retrieval Algorithm

Yi Xiong, Ravi Kumar, and Chenggen Quan

Department of Mechanical Engineering, National University of Singapore, Singapore 117576

DOI:10.1109/JPHOT.2019.2936236

Manuscript received August 8, 2019; accepted August 14, 2019. Date of publication August 20, 2019; date of current version September 19, 2019. This work was supported by the National University of Singapore under Research Project R-265-000-589-114. Corresponding author: Chenggen Quan (email: mpeqcg@nus.edu.sg).

Abstract: In this paper, the security of the cryptosystem based on phase-truncation Fourier transform (PTFT) and Gerchberg-Saxton (G-S) algorithm is analyzed. In this cryptosystem, the phase key generated using phase-truncated (PT) operation is bonded with the phase key generated in G-S algorithm to form the first private key, which improves the complexity of the first private key. In addition, since the second private key is generated using the G-S algorithm, the number of known constraints decreases compared to the traditional PTFT-based cryptosystem, which will lead the non-convergence of special attacks. However, it has been found that two private keys generated in the cryptosystem based on PTFT and G-S algorithm are related to one phase key generated in the G-S algorithm, which provides an additional constraint to retrieve the other private key when one private key is disclosed. Based on this analysis, two iterative processes with different constraints are proposed to crack the cryptosystem based on PTFT and G-S algorithm. This is the first time to report the silhouette problem existing in the cryptosystem based on PTFT and G-S algorithm. Numerical simulations are carried out to validate the feasibility and effectiveness of our analysis and proposed iterative processes.

Index Terms: Optical image encryption and authentication, security analysis, silhouette problem.

1. Introduction

Information security and authentication have attracted increasing attention in recent decades because of the rapid development of computer techniques and the wide use of the internet. Due to their unique advantages, such as parallel processing and multidimensional capabilities, optical techniques have been introduced in the field of information security [1]–[3]. A well-known optical encryption technique named double random phase encoding (DRPE) in which the input image is encoded into a noise-like image by using two independent random phase-only masks (RPMs) located at the input (spatial) and Fourier (frequency) planes, respectively, was proposed by Refregier and Javidi [4]. Subsequently, a large number of image encryption systems based on optical techniques, such as digital holography [5], [6], phase shifting [7], [8], diffractive imaging [9], [10], interference [11], [12] and polarization [13], [14], have been proposed. Simultaneously, cryptoanalysis on existing encryption schemes has been also proposed to disclose their inherent drawbacks [15]–[25] and promote the investigation of advanced and security-enhanced cryptosystems [26]–[30]. For example, it has been found that the DRPE-based cryptosystem [4] is vulnerable to some attacks, such as chosen-ciphertext [15], [16] and known-plaintext attacks [17], due to its inherent linearity. To address this issue, some techniques, such as equal modulus decomposition [26], scrambling algorithms [28] and ghost imaging [29], have been introduced to enhance the system security; however, the additional algorithms increase the difficulty of fully optical implementation for the security-enhanced cryptosystems.

Qin and Peng proposed a PTFT-based cryptosystem in which two RPMs regarded as private keys in the DRPE-based cryptosystem are used as public keys while two private keys are generated in the encryption process by using PT operations [31]. It seems that PT operations can remove the linearity of the DRPE-based structure, which makes PTFT-based cryptosystem immune to the attacks that the DRPE-based structure is vulnerable to; however, it is found that the PTFT-based structure is vulnerable to some special attacks due to enough constraints provided by two public keys [32], [33]. In addition, it is also found that most information of the plaintext could be retrieved when the first private key is known even without any knowledge of the corresponding ciphertext and the second private key [25]. The silhouette problem caused by the first private key in the PTFT-based cryptosystem will lead to serious information disclosure, which needs to be further enhanced. Rajput and Nishchal proposed a nonlinear G-S algorithm based optical image encryption scheme in which two private keys are generated in the encryption process by using G-S phase retrieval algorithm twice and the decryption process is performed using conventional DRPE-based architecture [34]. The G-S phase-retrieval algorithm-based cryptosystem has high robustness against most of the existing attacks, i.e., known-plaintext, chosen-plaintext and special attacks. Subsequently, Rajput and Nishchal proposed an optical encryption and authentication scheme based on the PTFT and G-S algorithm [35]. In this cryptosystem, the first private key is formed by combining the phase key obtained by the PT operation with the phase key obtained by the G-S algorithm. Compared to the traditional PTFT-based cryptosystem [31] in which the first private key is directly obtained using the first PT operation, the first private key in the cryptosystem [35] is more complex. Besides, compared to the conventional PTFT-based scheme in which the second private key is generated by the second PT operation, the second private key in the cryptosystem [35] is generated directly in the G-S iterative process, which has higher robustness against most of the existing attacks. It seems that the security level of the cryptosystem [35] has been improved due to the security enhancement of the private keys. However, based on our analysis, it is found that two private keys are relative to one phase key generated in the G-S iterative process; consequently, it appears possible that the other private key could be retrieved with the knowledge of one private key. Partial information of plaintexts could be retrieved using the retrieved private keys, which means the silhouette problem caused by two private keys exists in the cryptosystem based on PTFT and G-S algorithm.

In this paper, the security of the cryptosystem based on the PTFT and G-S algorithm is evaluated. The rest of this paper is organized as follows. In Section 2, the scheme under study is introduced briefly. In Section 3, the principle of two iterative processes with different constraints used to crack the cryptosystem [35] is introduced, and the feasibility and effectiveness of the proposed iterative processes are validated by numerical simulations. In Section 4, the concluding remarks are given.

2. The Scheme Under Study

The flow chart of the encryption and authentication process in the scheme [35] under study is shown in Fig. 1. The function $f_n(x, y)$ is the nth input image to be encrypted and verified, where $n = 1, 2, 3 \ldots$. Functions $R_1(x, y)$ and $R_2(u, v)$ are two independent RPMs distributed uniformly in the interval $[0, 2\pi]$. Function $R(x, y)$ is the random mask distributed uniformly in the interval [0, 1]. The phase key $P_{1n}(u, v)$ used to form the first private key is generated in the PTFT-based structure given by

$$\begin{cases} A_{1n}(u, v) = PT\{FT[f_n(x, y) R_1(x, y)]\}, \\ P_{1n}(u, v) = AT\{FT[f_n(x, y) R_1(x, y)]\}, \end{cases} \tag{1}$$

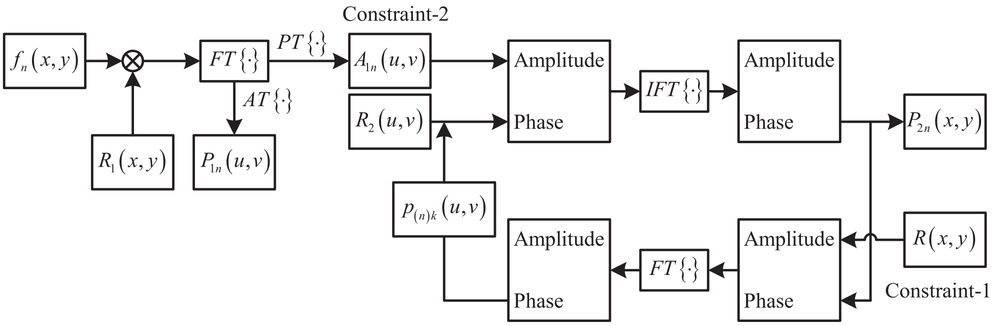


Fig. 1. The schematic diagram of the encryption and authentication process in [35].

where $FT\{\cdot\}$ denotes the Fourier transform, $PT\{\cdot\}$ and $AT\{\cdot\}$ denote the phase- and amplitude-truncated operators, respectively. $A_{1n}(u, v)$ and $P_{1n}(u, v)$ are the amplitude and phase parts of the Fourier spectrum, respectively. $A_{1n}(u, v)$ is used as the input of the phase-retrieval technique-based iterative process to generate the second private key. Now, using RPM, $R_2(u, v)$ as the initial phase distribution in the Fourier plane at $k = 1$, the iterative process is carried out as follows:

1) The phase distribution in the image plane after *kth* ($k \geq 1$) iteration is given by

$$P_{2(n)k}(x, y) = AT\left\{IFT\left[A_{1n}(u, v)\, p_{(n)(k-1)}(u, v)\right]\right\}, \tag{2}$$

where $IFT\{\cdot\}$ denotes the inverse Fourier transform, $P_{2(n)k}(x, y)$ and $p_{(n)k}(u, v)$ are the phase distributions in the image and Fourier planes at the *kth* iteration, respectively.

2) The random mask $R(x, y)$ is used as the amplitude constraint and boned with $P_{2(n)k}(x, y)$, $p_{(n)k}(u, v)$ is given by

$$p_{(n)k}(u, v) = AT\left\{FT\left[R(x, y)\, P_{2(n)k}(x, y)\right]\right\}, \tag{3}$$

where $p_{(n)k}(u, v)$ is used to update the phase distribution in the Fourier plane at the $(k+1)$*th* iteration.

Steps 1–2 are iterated until the correlation coefficient (CC) value reached the preset threshold value. The private key $p_n(u, v)$ used to form the first private key and $P_{2n}(x, y)$ used as the second private key are the outputs of the iterative process. The CC value between $R(x, y)$ and $g_{(n)k}(u, v) = PT\{IFT[A_{1n}(u, v)p_{(n)(k-1)}(u, v)]\}$ is given by

$$\mathrm{CC} = \frac{\mathrm{cov}\left(R, g_{(n)k}\right)}{\left(\sigma_R, \sigma_{g_{(n)k}}\right)}, \tag{4}$$

where cov$\{\cdot\}$ denotes the cross-covariance, and σ denotes the standard deviation (the coordinates of the function are omitted here for brevity).

In the decryption and verification process, the decrypted image $d_n(x, y)$ is given by

$$d_n(x, y) = PT\left\{IFT\left\{FT\left[R(x, y)\, K_{2n}(x, y)\right] K_{1n}(u, v)\right\}\right\}, \tag{5}$$

where $conj\{\cdot\}$ denotes a complex conjugate, two asymmetric phase keys $K_{1n}(u, v)$ and $K_{2n}(x, y)$ formed by three phase keys ($P_{1n}(u, v)$, $p_n(u, v)$ and $P_{2n}(x, y)$) generated in the encryption process are given by

$$\begin{cases} K_{1n}(u, v) = P_{1n}(u, v)\, conj\left[p_n(u, v)\right] \\ K_{2n}(x, y) = P_{2n}(x, y) \end{cases} \tag{6}$$

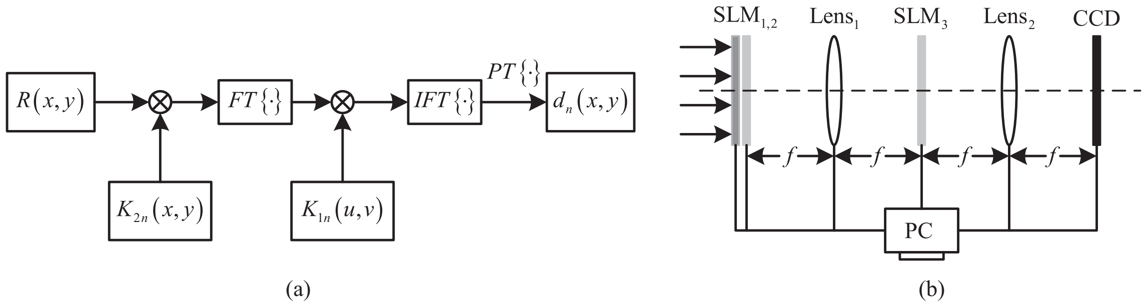


Fig. 2. (a) The schematic diagram of the decryption and verification process in [35]. (b) The schematic diagram of the optical setup for the decryption and verification process in [35].

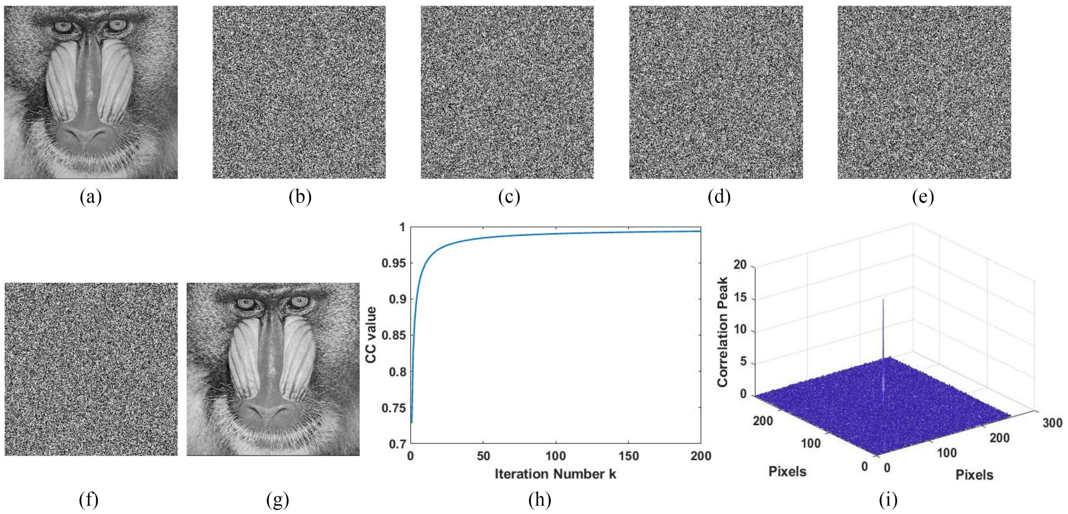


Fig. 3. (Color online) Simulation results for the gray- scale image ‘baboon’. (a) The original gray-scale input image ($f_1(x, y)$) to be verified. (b) The random mask $R(x, y)$. (c) The RPM $R_1(x, y)$. (d) The RPM $R_2(u, v)$. (e) The private key $K_{11}(u, v)$. (f) The private key $K_{21}(x, y)$. (g) The retrieved gray-scale image ($d_1(x, y)$). (h) The relation for matching of $R(x, y)$ with $A_{11}(u, v)$. (i) The auto-correction peak.

The nonlinear optical correlation (NOC) is implemented to achieve the information authentication and verification, which is given by

$$NOC(x, y) = IFT\left\{|FT[d_n(x, y)] \times FT[f_n(x, y)]|^t \times \exp\{i \arg[FT(d_n(x, y))] - \arg[FT(f_n(x, y))]\}\right\}, \tag{7}$$

where t is the nonlinearity factor and we have used $t = 0.3$ in our simulations. arg$\{\cdot\}$ is the operation to obtain the complex angle.

The schematic diagram of the decryption and verification process is shown in Fig. 2(a). On the other hand, the decryption and verification process can be achieved optically by employing the DRPE-based scheme. The random mask $R(x, y)$ displayed on the first spatial light modulator (SLM$_1$) is boned with the asymmetric phase key $K_{2n}(x, y)$ displayed on the SLM$_2$, and then is Fourier transformed. The Fourier spectrum boned with the asymmetric phase key $K_{1n}(u, v)$ displayed on the SLM$_3$ is then inversely Fourier transformed, and the final retrieved intensity pattern is displayed and recorded on the charge-coupled device (CCD) camera.

Numerical simulations are carried out to validate the feasibility and effectiveness of the cryptosystem in [35]. A gray-scale image ($f_1(x, y)$) with size of 256 × 256 pixels to be verified is shown in Fig. 3(a). Figs. 3(b)–(d) show the random mask ($R(x, y)$) fixed in the cryptosystem and two RPMs ($R_1(x, y)$ and $R_2(u, v)$), respectively. Figs. 3(e) and (f) show the asymmetric phase keys ($K_{11}(u, v)$

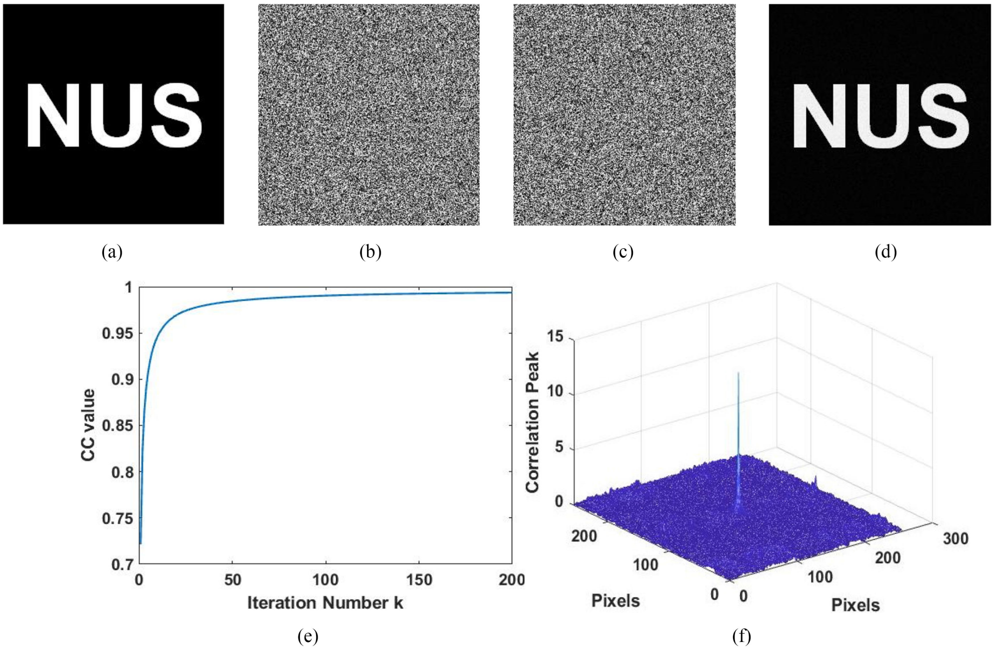


Fig. 4. (Color online) Simulation results for the binary image ‘NUS’. (a) The original binary input image ($f_2(x, y)$) to be verified. (b) The private key $K_{12}(u, v)$. (c) The private key $K_{22}(x, y)$. (d) The retrieved gray-scale image ($d_2(x, y)$). (e) The relation for matching of $R(x, y)$ with $A_{12}(u, v)$. (f) The auto-correction peak.

and $K_{21}(x, y)$) generated in the encryption process, respectively. From the simulation results shown in Figs. 3(b)–(f), no useful information of the original gray-scale image is visible. With the help of $R(x, y)$ and two asymmetric phase keys, the retrieved gray-scale image $d_1(x, y)$ is shown in Fig. 3(g). It can be seen that most information of the original image has been retrieved. The relation between CC values and iteration number k for matching of the random mask ($R(x, y)$) with the amplitude constraint of the phase-retrieval iterative process ($A_{11}(u, v)$) is shown in Fig. 3(h), from which it can be seen that a rapid convergence exists in the iterative process. The correlation value between the original gray-scale image in Fig. 3(a) and the retrieved image in Fig. 3(g) is shown in Fig. 3(i). It can be seen that an evident correlation peak exists, which means the retrieved image is authenticated. In addition, a binary image shown in Fig. 4(a) with the same size, which is encoded in the same random mask $R(x, y)$, is also used to validate the feasibility of the cryptosystem in [35]. The simulation results are shown in Fig. 4. From the simulation results in Figs. 3 and 4, it is shown that the cryptosystem in [35] can achieve encryption and authentication for several images. In addition, the authors [35] also claimed that the cryptosystem is free from special attacks which the traditional PTFT-based cryptosystem are vulnerable to.

3. Security Analysis

From the simulation results shown above, it can be seen that the gray-scale image ($f_1(x, y)$) and the binary image ($f_2(x, y)$) are authenticated by the same random mask ($R(x, y)$), which confirms the applicability of the scheme with different kind of images. Compared to the traditional PTFT-based cryptosystem [31] in which two cascaded PTFT-based structures are used to generate the private keys, the security level has been enhanced by combining a PTFT-based structure with a G-S iterative process. It has been found that most information of the plaintexts has been encoded into the first private key using the traditional PTFT-based cryptosystem [31]; consequently, most information of the plaintexts could be retrieved with the knowledge of the first private key even without any knowledge of the second private key and the corresponding ciphertexts [25]. In the cryptosystem based on PTFT and G-S iterative process, the phase key $P_{1n}(u, v)$ generated from the PTFT-based structure is bonded with the other phase key $p_n(u, v)$ to form the first private key $K_{1n}(u, v)$, which means that the phase key $P_{1n}(u, v)$ in which most information of the plaintexts is encoded is further encrypted. In addition, compared to the traditional PTFT-based cryptosystem in which the amplitude part of the Fourier spectrum is encoded and the second private key is generated by the second PTFT-based structure, some information encoded into the amplitude part of the Fourier spectrum ($A_{1n}(u, v)$) is further encoded using the G-S iterative process from which the second private key $K_{2n}(x, y)$ or $P_{2n}(x, y)$ is generated in the cryptosystem based on PTFT and G-S algorithm. The processes which are used to generate the second private key in the traditional PTFT-based cryptosystem [31] and the cryptosystem in [35] can be respectively described as

$$IFT\left[A_{1n}(u, v) R_2(u, v)\right] = C_n(x, y) P_{2n}(x, y), \tag{8}$$

$$IFT\left[A_{1n}(u, v) p_n(u, v)\right] = R(x, y) P_{2n}(x, y), \tag{9}$$

where $C_n(x, y)$ is the ciphertext generated using the traditional PTFT-based cryptosystem. In the cryptography, it is assumed that the attacker has access to the encryption algorithm and some sources, such as public keys, pairs of plaintexts and the corresponding ciphertexts. In the Eq. (8), $C_n(x, y)$ used as the ciphertext and $R_2(u, v)$ used as the public key are known, which makes possible to retrieve the amplitude part of the Fourier spectrum $A_{1n}(u, v)$ and the second private key $P_{2n}(x, y)$. The relation between the input and the output of the G-S algorithm with enough iterations is described as Eq. (9). Since $p_n(u, v)$ generated in the iterative process is unknown, it is impossible to retrieve $A_{1n}(u, v)$ and $P_{2n}(x, y)$ even with the knowledge of the random mask $R(x, y)$. Consequently, the security level of the cryptosystem based on the PTFT and G-S algorithm has been enhanced.

However, it is noteworthy that $R(x, y)$ is not directly related to the plaintexts, which means that most information of the plaintexts has not been encoded into $R(x, y)$. Hence, most information of the plaintexts could be retrieved even without any knowledge of $R(x, y)$. In addition, it can be seen that two private keys ($K_{1n}(u, v)$ and $K_{2n}(x, y)$) are related to $p_n(u, v)$ generated in the G-S algorithm, partial information of the private keys can be obtained if $p_n(u, v)$ could be retrieved; hence, the information of plaintexts could be retrieved using the retrieved private keys. In this study, the silhouette problem existing in the cryptosystem based on PTFT and G-S algorithm has been found. In addition, since the second private key $K_{2n}(x, y)$ has low sensitivity, the security of the cryptosystem needs to be further improved. To the best of our knowledge, it is the first time that the cryptoanalysis to attack the encryption scheme based on PTFT and G-S algorithm has been proposed.

3.1 Silhouette Problem Caused by the Second Private Key

During the decryption process of the cryptosystem in [35], the random mask $R(x, y)$, the second private key $K_{2n}(x, y)$ and the first private key $K_{1n}(u, v)$ are needed to obtain the decoded image according to Eq. (5). As mentioned above, $R(x, y)$ is unrelated to the plaintexts while all information of plaintexts are encoded into $K_{1n}(u, v)$ and $K_{2n}(x, y)$. Hence, the cryptoanalysis on the private keys generated in the encryption process is carried out.

With the knowledge of the private key $K_{2n}(x, y)$, the information of the plaintext can be retrieved using the proposed iterative process in Fig. 5. The iterative process can be carried out as follows:

1) At the *kth* iteration, an estimated random mask $R'_k(x, y)$ boned with the correct key $K_{2n}(x, y)$ is Fourier transformed, then the estimated phase and amplitude parts on the Fourier plane are given by

$$\begin{cases} g'_{(n)k}(u, v) = PT\left\{FT\left[R'_k(x, y) K_{2n}(x, y)\right]\right\}, \\ p'_{(n)k}(u, v) = AT\left\{FT\left[R'_k(x, y) K_{2n}(x, y)\right]\right\}, \end{cases} \tag{10}$$

where $g'_{(n)k}(u, v)$ and $p'_{(n)k}$ are the estimated amplitude and phase parts of the Fourier spectrum at the *kth* iteration, respectively. We would like to emphasize that the simulation results

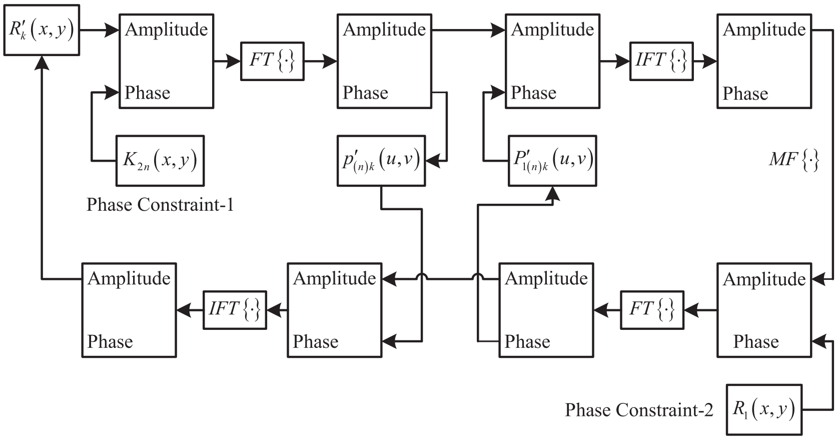


Fig. 5. The schematic diagram of the proposed iterative process with correct $K_{2n}(x, y)$.

shown in this study are obtained using randomly generated matrices ($R'_k(x, y)$, $P'_{1(n)k}(u, v)$ and $K'_{2(n)k}(x, y)$ in Section 3.2) as the initial conditions ($k = 1$). It is noteworthy that these matrices can also be fixed values when $k = 1$, such as $R'_k(x, y) = 0$ or $R'_k(x, y) = 1$. The similar simulation results will be obtained.

2) The estimated amplitude part in the Fourier plane $g'_{(n)k}(u, v)$ bonded with the estimated private key $P'_{1(n)k}(u, v)$ is inversely Fourier transformed, then the estimated amplitude part obtained on the image plane is given by

$$d''_{(n)k}(x, y) = PT\left\{IFT\left[g'_{(n)k}(u, v)\, P'_{1(n)k}(u, v)\right]\right\}, \tag{11}$$

3) The estimated plaintext $d'_{(n)k}(x, y)$ is given by

$$d'_{(n)k}(x, y) = MF\left[d''_{(n)k}(x, y)\right], \tag{12}$$

where $MF\{\cdot\}$ denotes a median filter.

4) The new estimated amplitude and phase parts on the Fourier plane are respectively given by

$$\begin{cases} g''_{(n)k}(u, v) = PT\left\{FT\left[d'_{(n)k}(x, y)\, R_1(x, y)\right]\right\}, \\ P'_{1(n)(k+1)}(u, v) = AT\left\{FT\left[d'_{(n)k}(x, y)\, R_1(x, y)\right]\right\}, \end{cases} \tag{13}$$

where $g''_{(n)k}(u, v)$ and $P'_{1(n)(k+1)}(u, v)$ are the new estimated amplitude and phase parts on the Fourier plane, respectively. $P'_{1(n)(k+1)}(u, v)$ is updated and used in step 2 at the $(k + 1)th$ iteration.

5) The new estimated random mask $R'_{(k+1)}(x, y)$ is given by

$$R'_{(k+1)}(x, y) = PT\left\{IFT\left[g''_{(n)k}(u, v)\, p'_{(n)k}(u, v)\right]\right\}, \tag{14}$$

where $R'_{(k+1)}(x, y)$ is updated and used as the input of the iterative process at $(k + 1)th$ iteration.

Steps 1–5 are iterated until the number of iterations k reached the preset value. Numerical simulations are carried out using MATLAB R2018b (on an Intel Core i5-4570 3.20 GHz, RAM 8 GB PC) to examine the feasibility and effectiveness of the proposed iterative process. Employing the proposed iterative process in Fig. 5 and with knowledge of the correct $K_{21}(x, y)$, the retrieved gray-scale image ($d'_1(x, y)$) is shown in Fig. 6(a). It can be seen that most information of the gray-scale image ($f_1(x, y)$) has been retrieved even though the retrieved image is blurred. The relation between CC values and the number of iterations k for matching $d'_1(x, y)$ and $f_1(x, y)$ is shown in Fig. 6(b), from which it can be seen that the CC values reach close to 0.7 within a few iterations. The computational time for 200 iterations is 10.0351 seconds. The auto-correlation value between $d'_1(x, y)$ with 200 iterations and $f_1(x, y)$ is shown in Fig. 6(c). An evident peak exists in the noisy background, which means the retrieved gray-scale image is successfully verified. From the simulation results shown

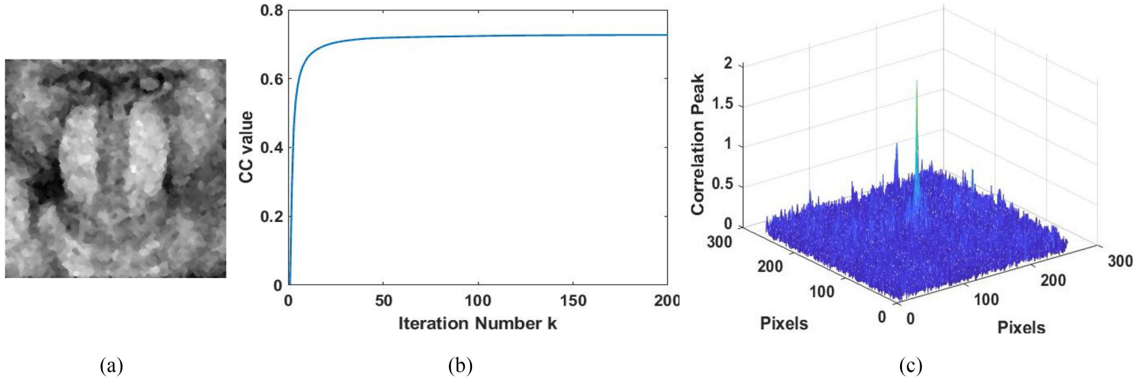


Fig. 6. (Color online) Simulation results of the proposed iterative process with correct $K_{21}(x, y)$ on the cryptosystem [35]. (a) The retrieved gray-scale image ($d'_1(x, y)$) obtained using the proposed attack with 200 iterations. (b) The relation between CC values and iteration number k for matching $d'_1(x, y)$ and Fig. 3(a). (c) The auto-correction peak.

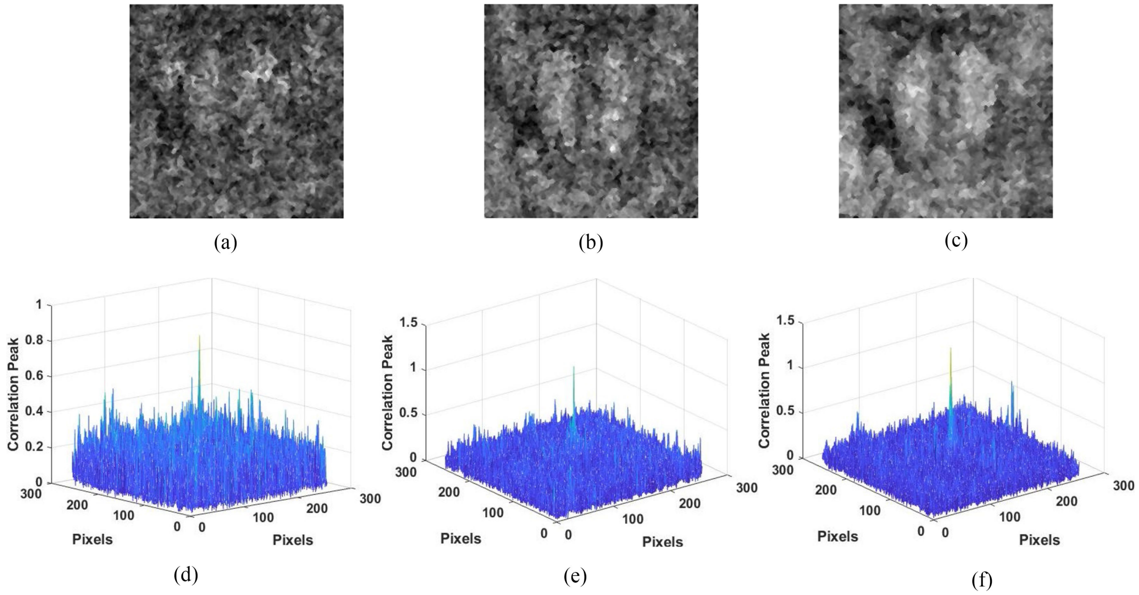
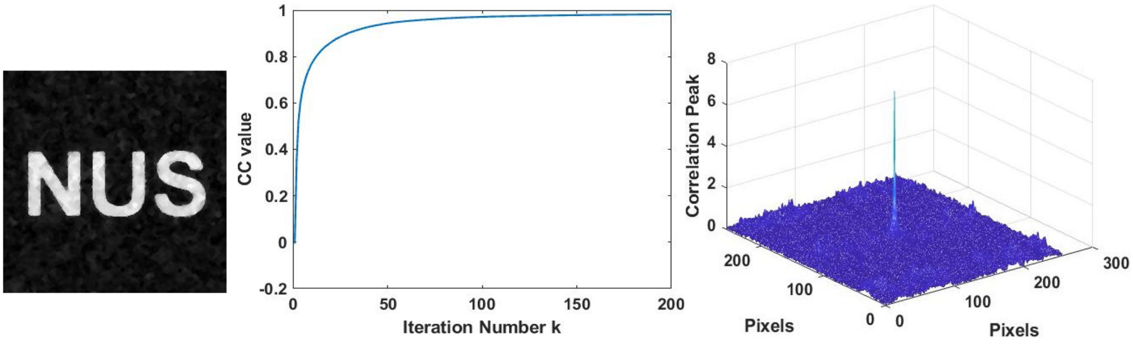


Fig. 7. (Color online) Simulation results of the proposed iterative process with partially correct $K_{21}(x, y)$ on the cryptosystem [35]. (a)-(c) $d'_1(x, y)$ obtained using the proposed attack with 85%, 90% and 95% correct $K_{21}(x, y)$, respectively. (d)-(f) The auto-correlation peaks obtained using the proposed attack with 85%, 90% and 95% correct $K_{21}(x, y)$, respectively.

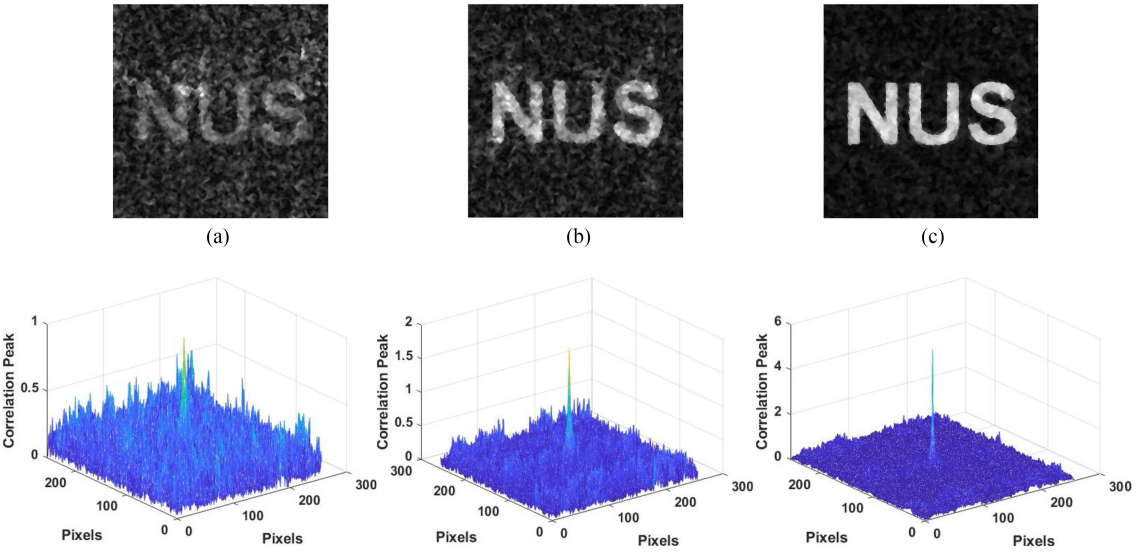
in Fig. 6, it can be seen the information of $f_1(x, y)$ can be retrieved using the proposed iterative process with $K_{21}(x, y)$, which means that the silhouette information of plaintexts will be disclosed when some information of the second private key leaks.

In addition, to further validate that the silhouette problem existing in the cryptosystem which would be caused by the partial information of $K_{2n}(x, y)$ known by the unauthorized user, simulations with partially known $K_{2n}(x, y)$ is carried out and the corresponding results are shown in Fig. 7. The retrieved grayscale images obtained using the proposed iterative process with 85%, 90% and 95% correct $K_{21}(x, y)$ are shown in Figs. 7(a)–(c), respectively. The auto-correlation values between retrieved images obtained using the proposed iterative process with 85%, 90% and 95% correct $K_{21}(x, y)$ and $f_1(x, y)$ are shown in Figs. 7(d)–(f), respectively. From simulation results in Fig. 7, it is shown that the retrieved grayscale-image has lower quality when the less information of



(a) (b) (c)

Fig. 8. (Color online) Simulation results of the proposed iterative process with correct $K_{22}(x, y)$ on the cryptosystem [35]. (a) The retrieved gray-scale image ($d'_2(x, y)$) obtained using the proposed attack with 200 iterations. (b) The relation between CC values and iteration number k for matching $d'_2(x, y)$ and Fig. 4(a). (c) The auto-correction peak.



(a) (b) (c)

(d) (e) (f)

Fig. 9. (Color online) Simulation results of the proposed iterative process with partially correct $K_{22}(x, y)$ on the cryptosystem [35]. (a)–(c) $d'_2(x, y)$ obtained using the proposed attack with 85%, 90% and 95% correct $K_{22}(x, y)$, respectively, (d)–(f) The auto-correlation peaks obtained using the proposed attack with 85%, 90% and 95% correct $K_{22}(x, y)$, respectively.

$K_{21}(x, y)$ is known. However, auto-correlation peaks still exist when the partially correct information of $K_{21}(x, y)$ is used to retrieve the information, which means that the retrieved image obtained using the proposed iterative process can be verified successfully.

Similarly, a binary image is also considered to be retrieved using the proposed iterative process with correct $K_{22}(x, y)$ and the simulation results are shown in Fig. 8. Additionally, simulation with the partially correct $K_{22}(x, y)$ is carried out and the corresponding results are shown in Fig. 9. The computational time for 200 iterations is 9.9375 seconds. The simulation results shown in Figs. 8 and 9 are similar to the results shown in Figs. 6 and 7, respectively. Compared to the results shown in Fig. 7, the retrieved binary image has better quality than that of the gray-scale image even with less knowledge of $K_{2n}(x, y)$. It is shown that $K_{2n}(x, y)$ causes more serious silhouette problem when the cryptosystem [35] is used to encrypt and authenticate binary images.

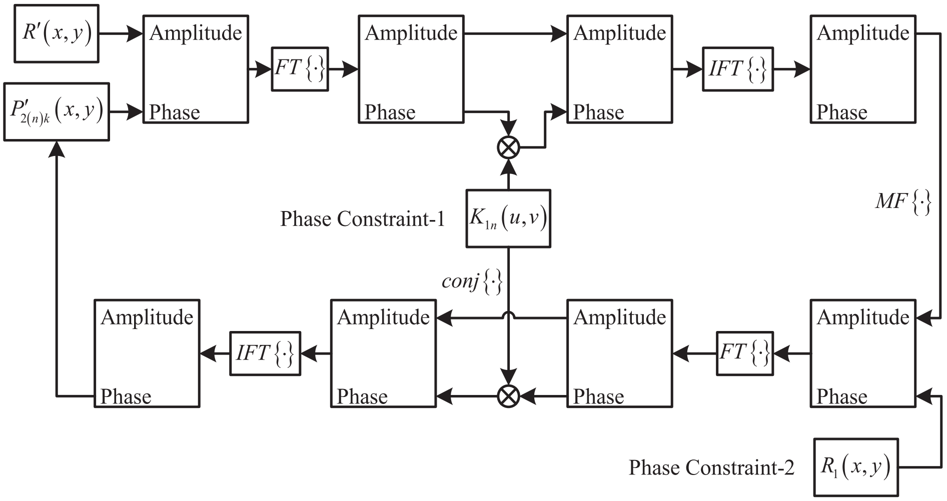


Fig. 10. The schematic diagram of the proposed iterative process with correct $K_{1n}(u, v)$.

From the simulation results shown, it can be seen that the information of plaintexts can be retrieved using the proposed iterative process with partially correct $K_{2n}(x, y)$ and without any knowledge of $K_{1n}(u, v)$ and the ciphertext $R(x, y)$. It is shown that the most information of $A_{1n}(u, v)$ has been encoded in $K_{2n}(x, y)$ using the phase-retrieval iterative process in cryptosystem [35], which may cause silhouette problem when the information of the private key $K_{2n}(x, y)$ leak.

3.2 Silhouette Problem Caused by the First Private Key

Since the phase part on the Fourier plane ($P_{1n}(u, v)$) is bonded with the phase key generated in the G-S algorithm ($p_n(u, v)$) to obtain the first private key $K_{1n}(u, v)$, most information of plaintexts encoded into $P_{1n}(u, v)$ are further encrypted. Compared to the traditional PTFT-based cryptosystem in which $P_{1n}(u, v)$ generated in the first PTFT-based structure is directly used as the first private key, the security level of the cryptosystem in [35] is higher. However, it can be seen that $K_{1n}(u, v)$ and $K_{2n}(x, y)$ are related to $p_n(u, v)$, which can be used as an additional constraint to retrieve $K_{2n}(x, y)$ with the knowledge of $K_{1n}(u, v)$. Employing the retrieved private keys, the information of the original images could be retrieved. In addition, since $R(x, y)$ is the ciphertext fixed in the cryptosystem and not relative to the plaintexts, $R(x, y)$ could be easily obtained by importing an arbitrary input to the cryptosystem according to the principle of cryptography. With the knowledge of the correct $K_{1n}(u, v)$, the information of plaintexts can be retrieved using the proposed iterative process shown in Fig. 10. The iterative process can be carried out as follows:

1) At the *kth* iteration, an estimated private key $K'_{2(n)k}(x, y)$ boned with the retrieved random mask $R'(x, y)$ is Fourier transformed, the amplitude and phase parts on the Fourier plane are respectively given by

$$g'_{(n)k}(u, v) = PT\left\{FT\left[R'(x, y)\,K'_{2(n)k}(x, y)\right]\right\}, \tag{15}$$

$$p'_{(n)k}(u, v) = AT\left\{FT\left[R'(x, y)\,K'_{2(n)k}(x, y)\right]\right\} \tag{16}$$

2) The estimated phase key $P'_{1(n)k}(u, v)$ is given by

$$P'_{1(n)k}(u, v) = K_{1n}(u, v)\,p'_{(n)k}(u, v), \tag{17}$$

3) Using the estimated phase key $P'_{1(n)k}(u, v)$ and the estimated amplitude part $g'_{(n)k}(u, v)$ obtained using Eq. (15), the estimated amplitude part on the input plane ($d'_{(n)k}(x, y)$) is

given by

$$d'_{(n)k}(x, y) = PT\left\{IFT\left[g'_{(n)k}(u, v)\,P'_{1(n)k}(u, v)\right]\right\}, \tag{18}$$

4) Employing a median filter on $d'_{(n)k}(x, y)$, a new estimated plaintext $d''_{(n)k}(x, y)$ is given by

$$d''_{(n)k}(x, y) = MF\left[d'_{(n)k}(x, y)\right], \tag{19}$$

5) Using the new estimated plaintext $d''_{(n)k}(x, y)$ and the public key $R_1(x, y)$, the new estimated amplitude and phase parts on the Fourier plane are respectively given by

$$\begin{cases} g''_{(n)k}(u, v) = PT\left\{FT\left[d''_{(n)k}(x, y)\,R_1(x, y)\right]\right\}, \\ P''_{1(n)k}(u, v) = AT\left\{FT\left[d''_{(n)k}(x, y)\,R_1(x, y)\right]\right\}, \end{cases} \tag{20}$$

where $g''_{(n)k}(u, v)$ and $P''_{1(n)k}(u, v)$ are the new estimated amplitude and phase parts of the Fourier spectrum, respectively.

6) The new estimated phase key $p''_{(n)k}(u, v)$ is given by

$$p''_{(n)k}(u, v) = P''_{1(n)k}(u, v)\{conj[K_{1n}(u, v)]\}, \tag{21}$$

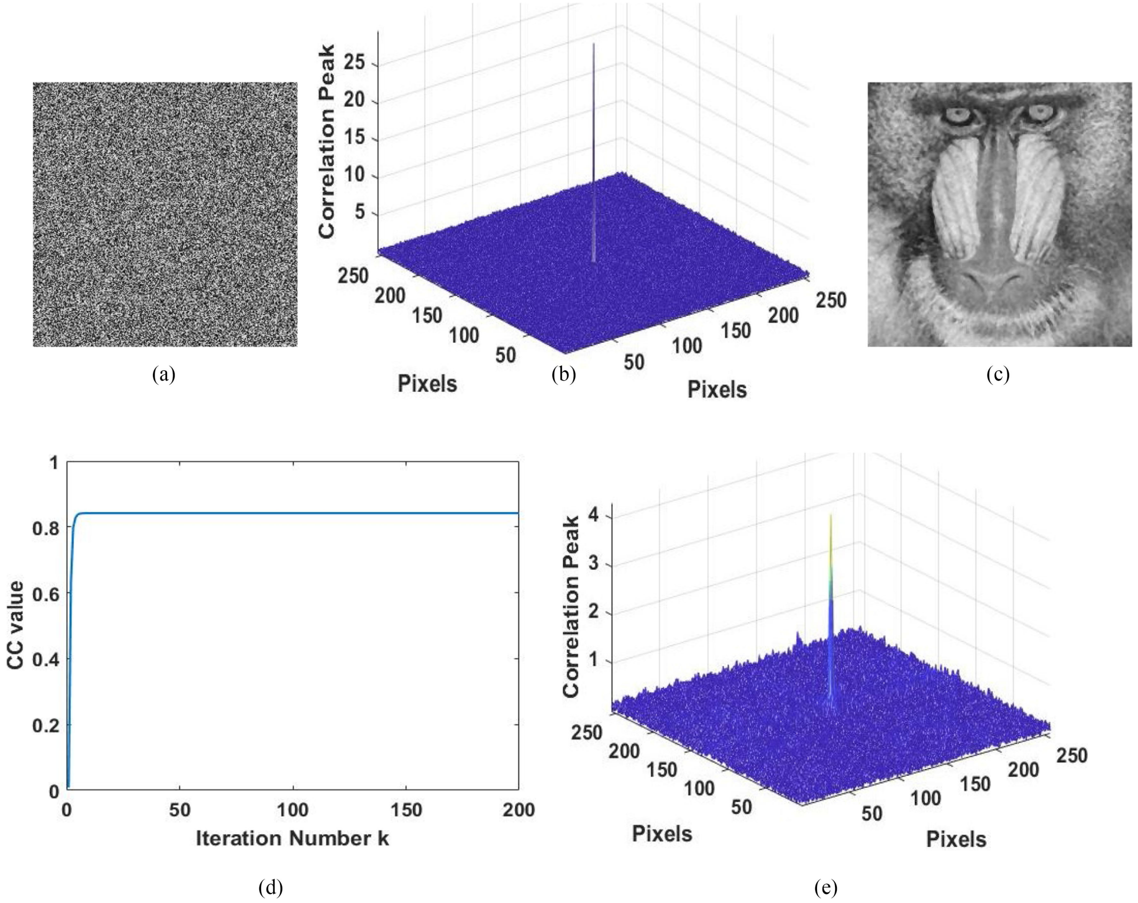
7. The new estimated private key $K'_{2(n)(k+1)}(x, y)$ is given by

$$K'_{2(n)(k+1)}(x, y) = AT\left\{IFT\left[g''_{(n)k}(u, v)\,p''_{(n)k}(u, v)\right]\right\}, \tag{22}$$

where $K'_{2(n)(k+1)}(x, y)$ is updated and used as the input of the iterative process in Fig. 10 at the $(k+1)th$ iteration.

Steps 1–7 are iterated until the number of iterations (k) reached the preset value. Numerical simulation is also carried out. The gray-scale image in Fig. 3(a) is used as the arbitrary input to be imported in the cryptosystem, the retrieved random mask $R'(x, y)$ is shown in Fig. 11(a) while the correlation value between $R'(x, y)$ and Fig. 3(b) is shown in Fig. 11(b). Using the proposed iterative process with $R'(x, y)$ and the correct $K_{11}(u, v)$, the retrieved gray-scale image $d'_1(x, y)$ is shown in Fig. 11(c). It can be seen that most information of the gray-scale plaintext is visible from $d'_1(x, y)$ and the computational time for 200 iterations is 10.8963 seconds. The relation between CC values and iteration number k for matching $d'_1(x, y)$ and Fig. 3(a) is shown in Fig. 11(d) while the correlation value between $d'_1(x, y)$ with 200 iterations and Fig. 3(a) is shown in Fig. 11(e). A correlation peak exists in the noisy background, which means $d'_1(x, y)$ has been verified successfully. Using $R'(x, y)$ and the known $K_{12}(u, v)$, the retrieved binary image $d'_2(x, y)$ is shown in Fig. 12(a). The relation between CC values and iteration number k for matching $d'_2(x, y)$ and Fig. 4(a) is shown in Fig. 12(b). An evident correlation peak exists in Fig. 12(c), which means that $d'_2(x, y)$ with 200 iterations is verified successfully. The computational time for 200 iterations is 11.0016 seconds. To further validate the multiuser capability of $R'(x, y)$, a new gray-scale image with size of 256 × 256 pixels shown in Fig. 13(a) is used to carry out the simulation. The private key $K_{13}(u, v)$ generated in the encryption process is shown in Fig. 13(b). Using the known $K_{13}(u, v)$ and $R'(x, y)$, the retrieved image $d'_3(x, y)$ is shown in Fig. 13(c). It can be seen that most information of $f_3(x, y)$ is retrieved. The relation between CC values and iteration number k for matching $d'_3(x, y)$ and $f_3(x, y)$ is shown in Fig. 13(d). It can be seen that the CC values quickly converge to 1, which shows the effectiveness of the proposed iterative process shown in Fig. 10. The auto-correlation value for matching $d'_3(x, y)$ with 200 iterations and $f_3(x, y)$ is shown in Fig. 13(e).

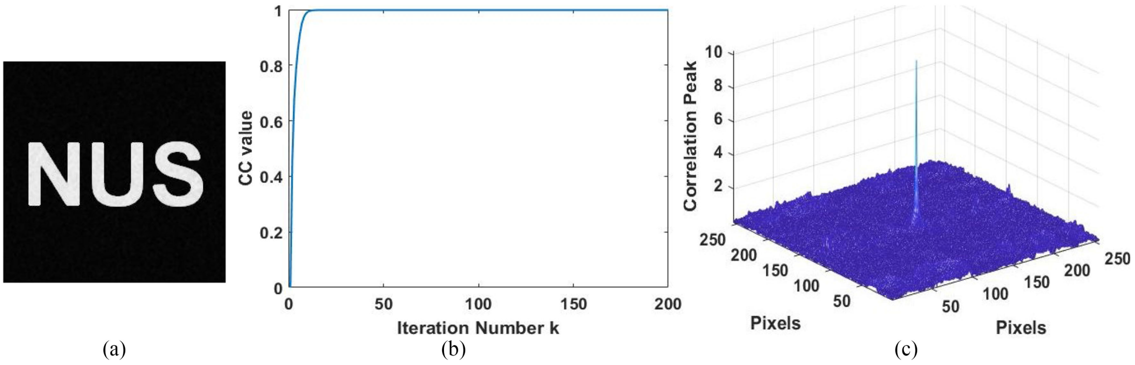
From the simulation results shown in Figs. 11–13, it can be seen that most information of the plaintexts can be retrieved using the proposed iterative process with the correct $K_{1n}(u, v)$ and without any knowledge of other private keys, which may cause the silhouette problem when the information of $K_{1n}(u, v)$ leak. Although the security level of $K_{1n}(u, v)$ has been enhanced, the dependent relation between two private keys provides an additional constraint to crack the cryptosystem. Thus, the cryptosystem in [35] needs to be further security enhanced.



(a) (b) (c)

(d) (e)

Fig. 11. (Color online) Simulation results of the proposed iterative process with correct $K_{11}(u, v)$ on the cryptosystem [35]. (a) The retrieved random mask $R'(x, y)$ obtained using Fig. 3(a) as the input of cryptosystem. (b) The auto-correlation peak between $R'(x, y)$ and $R(x, y)$. (c) The retrieved gray-scale image $d'_1(x, y)$ obtained using the proposed iterative process with 200 iterations. (d) The relation between CC values and iteration number k for matching $d'_1(x, y)$ and Fig. 3(a). (e) The auto-correction peak.



(a) (b) (c)

Fig. 12. (Color online) Simulation results of the proposed iterative process with correct $K_{12}(u, v)$ on the cryptosystem [35]. (a) The retrieved binary image $d'_2(x, y)$ obtained using the proposed iterative process with 200 iterations. (b) The relation between CC values and iteration number k for matching $d'_2(x, y)$ and Fig. 4(a). (c) The auto-correction peak.

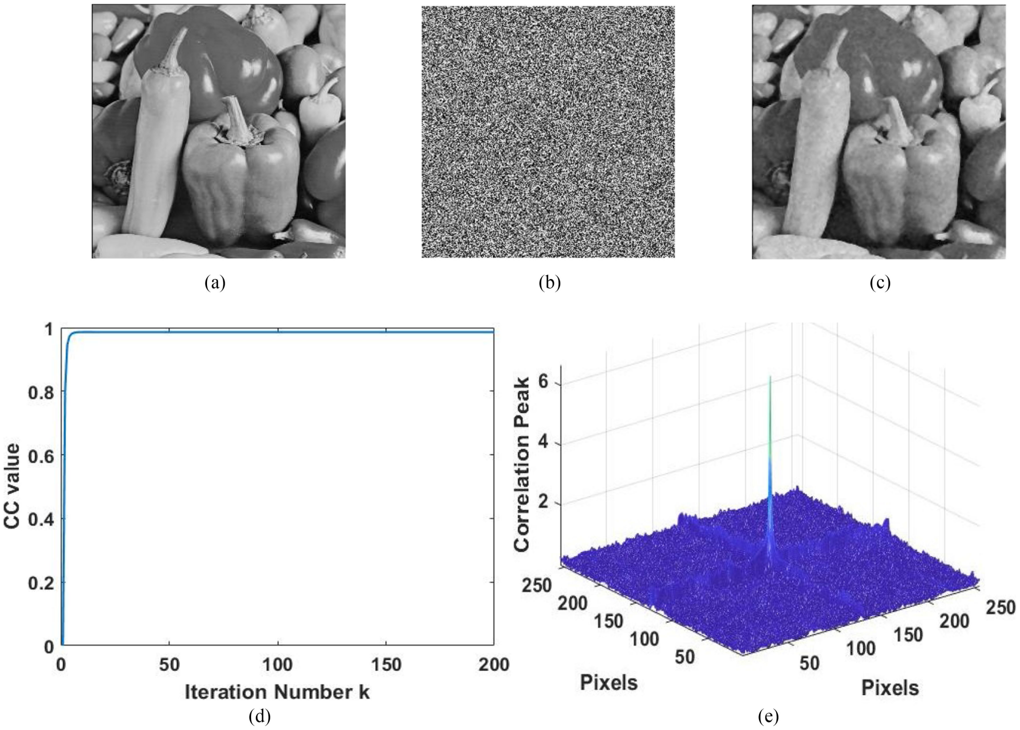


Fig. 13. (Color online) Simulation results of the proposed iterative process with correct $K_{13}(u, v)$ on the cryptosystem [35]. (a) The gray-scale image $f_3(x, y)$ to be retrieved. (b) The known private key $K_{13}(u, v)$. (c) The retrieved image $d'_3(x, y)$ obtained using the proposed iterative process with Fig. 11(a) an Fig. 13(b). (d) The relation between CC values and iteration number k for matching $d'_3(x, y)$ and $f_3(x, y)$. (e) The auto-peak.

4. Conclusions

In this paper, the security of the cryptosystem based on the PTFT and G-S algorithm has been analyzed. Since one random mask is used as the ciphertext for different plaintexts in the cryptosystem, the most information of the plaintexts has not been encoded into the random mask. Consequently, the security level of the cryptosystem based on the PTFT and G-S algorithm depends on the storage and transmission of two private keys generated in the encryption process. However, since two private keys are related to the phase key $p_n(u, v)$, it provides an additional constraint for attackers to retrieve the other private key and the corresponding plaintext with the knowledge of one private key. In this paper, two iterative processes with different constraints have been proposed to crack the cryptosystem based on PTFT and G-S algorithm successfully. Although the cryptosystem is immune to the special attack which the PTFT-based cryptosystem is vulnerable to, it has been found that the silhouette problem caused by two private keys exists, which would cause serious security problem if the information of any private key leak. In addition, it has been found that silhouette information of the plaintexts could be retrieved even when only partial information of the second private key is known; thus, the security level of the cryptosystem based on PTFT and G-S algorithm needs to be further enhanced. To the best of our knowledge, this is the first time that the silhouette problem existing in the cryptosystem based on PTFT and G-S algorithm is reported. Numerical simulation results validate the feasibility and effectiveness of our proposed iterative processes.

References

[1] B. L. Volodin, B. Kippelen, K. Meerholz, B. Javidi, and N. Peyghambarian, “A polymeric optical pattern-recognition system for security verification,” *Nature*, vol. 383, no. 6595, pp. 58–60, Sep. 1996.

[2] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, “Multiplexing encrypted data by using polarized light,” *Opt. Commun.*, vol. 260, pp. 109–112, Apr. 2006.
[3] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon.*, vol. 6, no. 7, pp. 120–155, Jun. 2014.
[4] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, pp. 767–769, Apr. 1995.
[5] B. Javidi and T. Nomura, “Securing information by use of digital holography,” *Opt. Lett.*, vol. 25, no. 1, pp. 28–30, Jan. 2000.
[6] E. Tajahuerce and B. Javidi, “Encrypting three-dimensional information with digital holography,” *Appl. Opt.*, vol. 39, no. 35, pp. 6595–6601, Dec. 2000.
[7] B. Hennelly and J. T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” *Opt. Lett.*, vol. 28, no. 4, pp. 269–271, Feb. 2003.
[8] X. F. Meng *et al.*, “Two-step phase-shifting interferometry and its application in image encryption,” *Opt. Lett.*, vol. 31, no. 10, pp. 1414–1416, May 2006.
[9] W. Chen and X. Chen, “Optical image encryption based on diffractive imaging,” *Opt. Lett.*, vol. 35, no. 22, pp. 3817–3819, Nov. 2010.
[10] Y. Qin, Q. Gong, and Z. Wang, “Simplified optical image encryption approach using single diffraction pattern in diffractive-imaging-based scheme,” *Opt. Exp.*, vol. 22, no. 18, pp. 21790–21799, Sep. 2014.
[11] Y. Zhang and B. Wang, “Optical image encryption based on interference,” *Opt. Lett.*, vol. 33, no. 21, pp. 2443–2445, Nov. 2008.
[12] N. Zhu, Y. Wang, J. Liu, J. Xie, and H. Zhang, “Optical image encryption based on interference of polarized light,” *Opt. Exp.*, vol. 17, no. 16, pp. 13418–13424, Aug. 2009.
[13] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, “Secure optical memory system with polarization encryption,” *Appl. Opt.* vol. 40, no. 14, pp. 2310–2315, May 2001.
[14] A. Alfalou and C. Brosseau, “Dual encryption scheme of images using polarized light,” *Opt. Lett.*, vol. 35, no. 13, pp. 2185–2187, Jul. 2010.
[15] 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, Jul. 2005.
[16] X. Peng, H. Wei, and P. Zhang, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” *Opt. Lett.* vol. 31, no. 22, pp. 3261–3263, Nov. 2006.
[17] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, “A known-plaintext heuristic attack on the Fourier plane encryption algorithm,” *Opt. Exp.*, vol. 14, no. 8, pp. 3181–3186, Apr. 2006.
[18] Y. Zhang, D. Xiao, W. Wen, and H. Liu, “Vulnerability to chosen-plaintext attack of a general optical encryption model with architecture of scrambling-then-double random phase encoding,” *Opt. Lett.*, vol. 38, no. 21, pp. 4506–4509, Nov. 2013.
[19] C. Zhang, M. Liao, W. He, and X. Peng, “Ciphertext-only attack on a joint transform correlator encryption system,” *Opt. Exp.*, vol. 21, no. 23, pp. 28523–28530, Nov. 2013.
[20] Y. Xiong, A. He, and C. Quan, “Security analysis of a double-image encryption technique based on an asymmetric algorithm,” *J. Opt. Soc. Amer. A*, vol. 35, no. 2, pp. 320–326, Feb. 2018.
[21] S. Jiao, G. Li, C. Zhou, W. Zou, and X. Li, “Special ciphertext-only attack to double random phase encryption by plaintext shifting with speckle correlation,” *J. Opt. Soc. Amer. A*, vol. 35, no. 1, pp. A1–A6, Jan. 2018.
[22] Y. Xiong, A. He, and C. Quan, “Hybrid attack on an optical cryptosystem based on phase-truncated Fourier transforms and a random amplitude mask,” *Appl. Opt.*, vol. 57, no. 21, pp. 6010–6016, Jul. 2018.
[23] Y. Xiong, A. He, and C. Quan, “Specific attack and security enhancement to optical image cryptosystem based on two random masks and interference,” *Opt. Lasers Eng.*, vol. 107, pp. 142–148, Aug. 2018.
[24] L. Wang, G. Li, Q. Wu, and G. Situ, “Cyphertext-only attack on the joint-transform-correlator-based optical encryption: Experimental demonstration,” *Appl. Opt.* vol. 58, no. 5, pp. A197–A201, Feb. 2019.
[25] Y. Xiong, A. He, and C. Quan, “Security analysis and enhancement of a cryptosystem based on phase truncation and a designed amplitude modulator,” *Appl. Opt.*, vol. 58, no. 3, pp. 695–703, Jan. 2019.
[26] G. Luan, A. Li, D. Zhang, and D. Wang, “Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain,” *IEEE Photon. J.*, vol. 11, no. 1, Dec. 2018, Art. no. 6900207.
[27] M. Shan, L. Liu, B. Liu, and Z. Zhong, “Security-enhanced optical interference-based multiple-image encryption using a modified multiplane phase retrieval algorithm,” *Opt. Eng.*, vol. 57, no. 8, Aug. 2018, Art. no. 083103.
[28] Y. Xiong, C. Quan, and C. J. Tay, “Multiple image encryption scheme based on pixel exchange operation and vector decomposition,” *Opt. Lasers Eng.*, vol. 101, pp. 113–121, Feb. 2018.
[29] S. Liansheng, W. Jiaohao, T. Ailing, and A. Asundi, “Optical image hiding under framework of computational ghost imaging based on an expansion strategy,” *Opt. Exp.*, vol. 27, no. 5, pp. 7213–7225, Mar. 2019.
[30] J. Chen, Y. Zhang, J. Li, and L. Zhang, “Security enhancement of double random phase encoding using rear-mounted phase masking,” *Opt. Lasers. Eng.*, vol. 101, pp. 51–59, Feb. 2018.
[31] W. Qin and X. Peng, “Asymmetric cryptosystem based on phase-truncated Fourier transforms,” *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, Jan. 2010.
[32] X. Wang and D. Zhao, “A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms,” *Opt. Commun.*, vol. 285, no. 6, pp. 1078–1081, Mar. 2012.
[33] Y. Wang, C. Quan, and C. J. Tay, “Improved method of attack on an asymmetric cryptosystem based on phase-truncated Fourier transform,” *Appl. Opt.* vol. 54, no. 22, pp. 6974–6881, Aug. 2015.
[34] S. K. Rajput and N. K. Nishchal, “Fresnel domain nonlinear optical image encryption scheme based on Gerchberg-Saxton phase-retrieval algorithm,” *Appl. Opt.*, vol. 53, no. 3, pp. 418–425, Jan. 2014.
[35] S. K. Rajput and N. K. Nishchal, “An optical encryption and authentication scheme using asymmetric keys,” *J. Opt. Soc. Amer. A*, vol. 31, no. 6, pp. 1233–1238, Jun. 2014.