IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 18, 2019, accepted December 6, 2019, date of publication December 12, 2019, date of current version January 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2959008

Nonlinear Double-Image Encryption in Cylindrical Diffraction-Based Scheme by Aid of Position Multiplexing

XIANGLING DING[1], YANMING HUANG[1], DENGYONG ZHANG[2], AND YUN SONG[2]
[1]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411004, China
[2]School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China

Corresponding author: Yun Song (sonie@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772087, in part by the Scientific Research Foundation of Hunan Provincial Education Department of China under Grant 19B199 and Grant 19B004, in part by the Doctoral Research Foundation of Hunan University of Science and Technology under Grant E51974, and in part by the ''Double First-Class'' International Cooperation and Development Scientific Research Project of Changsha University of Science and Technology under Grant 2018IC25.

ABSTRACT Conventional phase-truncation-based double-image encryption (PT-DIE) scheme suffers from the phase retrieval algorithm-based attack, and information disclosure issue. In this paper, we introduce cylindrical diffraction and position multiplexing into the PT-DIE scheme. Through position multiplexing, double-image are integrated together. Then the integrated image is encoded into a real-valued cyphertext and two phase-only keys (POKs) by cylindrical diffraction. The decrypted images are acquired with two POKs by inverse cylindrical diffraction, and because of that, the phase retrieval algorithm-based attack and the information disclosure issue have been thoroughly conquered from a theoretical and experimental point of view. Furthermore, the proposed scheme can be extended to encode multi-image without changing original system architecture, and incurring additional computing burden. Simulation results have been manifested the validity and the security of the proposed scheme.

INDEX TERMS Nonlinear images encryption, position multiplexing, cylindrical diffraction, information disclosure, phase retrieval attack.

I. INTRODUCTION

Optical information security has attracted wide research interests in the field of information security due to the superior capabilities of high-speed, parallelism, and high encryption dimension [1], [7]. Especially, the double random phase-encoding technique (DRPE) based on 4-f system, which was firstly designed by Refregier and Javidi in 1995 [8], are extensively studied in recent years. However, some research results have disclosed that the DRPE algorithm and its extended approaches [9]–[12] are prone to various attacks including the known-plaintext attack [13], the chosen-plaintext attack [14], and the chosen-cyphertext attack [15] because of its linear characteristics.

To withstand these attacks stemmed from linearity issue, nonlinear encryption algorithm based on the operation of phase-truncation was presented by Qin and Peng [16]. But, this method was fragile to the specific attack based on the iterative Fourier transforms [17]. Therefore, some improvement cryptosystem [18]–[22] have been proposed to resist specific attack. In these approaches, a novel double-image nonlinear encryption algorithm has been proposed by Wang and Zhao [18]. It was reported that double-image were one step encoded into a noisy image by the operation of phase-truncation of a joint Fourier transform. Subsequently, the authors introduce, for the first time, the concept of ''information disclosure'' in phase-truncation based cryptosystems [23]. That is, if the main information of the input plaintext can be obtained by using one part of keys or cyphertexts, the risk of information disclosure emerges. However, for phase-truncation-based double-image encryption (PT-DIE) scheme [18], when using the two phase keys, obtained in encryption procedure, with the absence of the cyphertext to reconstruct the plaintext, the problem of information disclosure really exists. Although its enhancements were proposed in [23], and [24], method in [23]

The associate editor coordinating the review of this manuscript and approving it for publication was Ramakrishnan Srinivasan.

encrypted two images separately rather than as a whole, while algorithm in [24] focused on color image encryption not for double-image.

Furthermore, though the PT-DIE scheme has been declared that it is not affected by some common attacks, a hybrid attack strategy [25] is implemented to recover the encrypted double-image by using the phase retrieval algorithm and the joint power spectrum. Moreover, since this strategy needs the original position parameters and the computation-intensive retrieval approach, we further proposed a simple public-key attack scheme [26]. In this method, two decryption keys are simply produced by the three public keys and arbitrary position parameters, followed by the approximate values of the original double-image. Subsequently, a generalized phase retrieval algorithm [27], and its enhancement version [28] with median filtering and normalization operation are further proposed to break this double-image cryptosystem. Therefore, a nonlinear double-image encryption algorithm that can have high resistance against the phase retrieval algorithm-based attacks [25]–[28] and is free of information disclosure simultaneously, has yet to be developed.

To address these two issues, a nonlinear double-image strategy based on cylindrical diffraction and position multiplexing is proposed. In the process of cylindrical diffraction, the input is represented as a cylinder object, while the intermediate surface is concentric cylinder. Consequently, the position-multiplexed double-image can be encoded through an asymmetric cylindrical diffraction with three random phase masks positioned on the input and intermediate surfaces. Meanwhile, the operation of phase-truncation is employed on the intermediate and output surfaces, accompanied with two asymmetric phase-only masks for decryption and a real-valued amplitude cyphertext. In addition, the radius and the height of the cylinder plus the distance of the cylindrical diffraction can be employed as additional keys into the cryptosystem to further enhance the security of the system. The integration of phase-truncation maintains the properties of nonlinear structure, and it results in real-valued output. The deploying of cylindrical-diffraction helps to resist the phase retrieval algorithm-based attacks. Moreover, because of the asymmetric structure of cylindrical diffraction and inverse cylindrical diffraction, the issue of information disclosure is conquered. Numerical simulations are presented to validate the feasibility and effectiveness of the proposed cryptosystem. In [31], a cascade and independent encrypted cylindrical-diffraction scheme is proposed. However, in this paper, we extends that work in three ways. First, position multiplexing technique is adopted to fuse the double-image even multi-image as a whole, not in separate operation with the cascade mode. Second, this paper not only describes the cylinder diffraction can resist the phase retrieval attack and information disclosure from the experimental point of view, but also analyzes its feasibility from the theoretical point of view. Third, the proposed scheme does not need modify the system architecture to further encrypt multi-image as a whole. As a consequence, the multi-image can be encoded without extra time increasing, and decoded results do not appear the loss of quality.

The contributions of this paper are composed of four parts.

First, this is the first time in presenting a PT-DIE scheme that combines a position multiplexing technique together with a cylindrical-diffraction architecture. So, it holds the nonlinear property and asymmetric structure.

Second, the position multiplexing operation does not alter the cylindrical-diffraction setup of any kind. Thus, the encryption time of the proposed scheme has barely increased with the increment of images, and the quality of decrypted images is maintained.

Third, the procedure of encryption can be performed in one-step, avoiding objects locating procedure in cascaded cryptosystem. In this sense, the double-image even multi-image can be encoded simultaneously.

Four, the phase retrieval algorithm-based attack and the information disclosure issue have been conquered from a theoretical and experimental point of view.

II. THEORETICAL ANALYSIS

A. THE PT-DIE AND ITS SECURITY PROBLEMS

In PT-DIE, two plaintexts $f_1(x, y)$, and $f_2(x, y)$ that located in two different space position (a_1, b_1), and (a_2, b_2) are modulated with two random phase masks RPM_1, and RPM_2, respectively. Thus the input image can be denoted as

$$f(x,y) = [f_1(x,y) \cdot RPM_1(x,y)] * \delta(x-a_1, y-b_1) + [f_2(x,y) \cdot RPM_2(x,y)] * \delta(x-a_2, y-b_2) \quad (1)$$

After the execution of joint Fourier transform and the phase truncation, the amplitude part and one phase-only key can be calculated as

$$\begin{aligned} g(u,v) &= Tr\{FT[f(x,y)]\} \\ P_0(u,v) &= Re\{FT[f(x,y)]\} \end{aligned} \quad (2)$$

where the operators $Tr\{\cdot\}$, $Re\{\cdot\}$ and $FT\{\cdot\}$ represent phase truncation, phase reservation, and Fourier transform, respectively.

In the same way, the final encrypted result $E(x)$ and another phase-only key can be obtained as

$$\begin{aligned} E(x,y) &= Tr\{IFT[g(u,v) \cdot RPM_3(u,v)]\} \\ P_1(x,y) &= Re\{IFT[g(u,v) \cdot RPM_3(u,v)]\} \end{aligned} \quad (3)$$

where $IFT\{\cdot\}$ and $RPM_3(u, v)$ are inverse Fourier transform and another random phase mask.

As reported in [18], using $P_0(u, v)$ and $P_1(x, y)$ as decryption keys and combining with the cyphertext, the plaintexts can be correctly retrieved. It is well known that there is an information disclosure issue existing in this cryptosystem [23]. In other words, some information about plaintext can be observed when using both $P_0(u, v)$ and $P_1(x, y)$ without the cyphertext in the verification scheme. Meanwhile, it has been reported that this scheme can be cracked by the phase retrieval algorithm-based attacks [25]–[28].

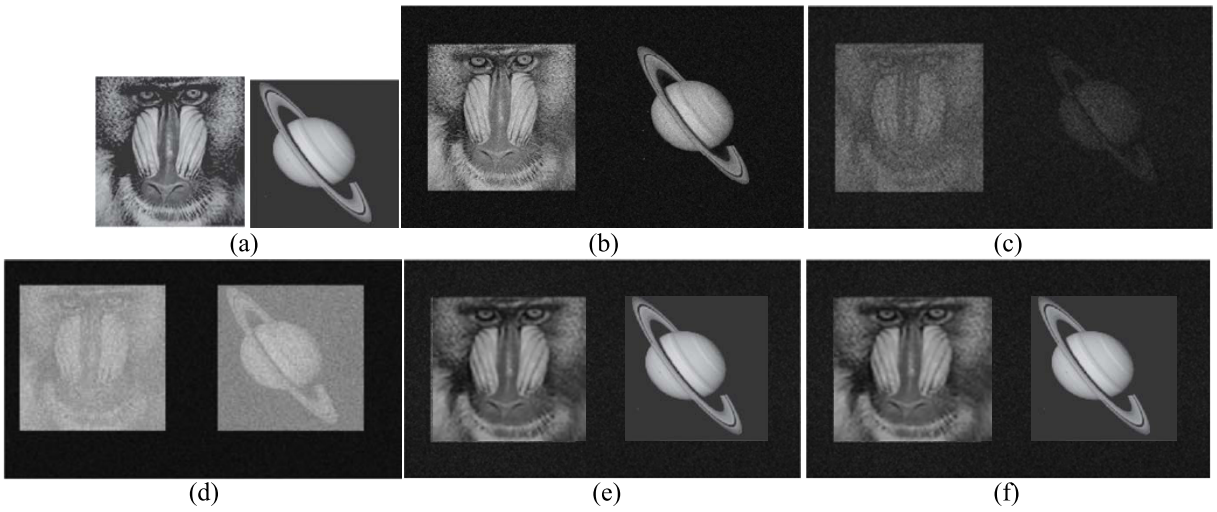

FIGURE 1. The input plaintexts (a), retrieved results (b) with disclosure of both $P_0(u, v)$ and $P_1(x, y)$, and the attacks results (c)-(f).

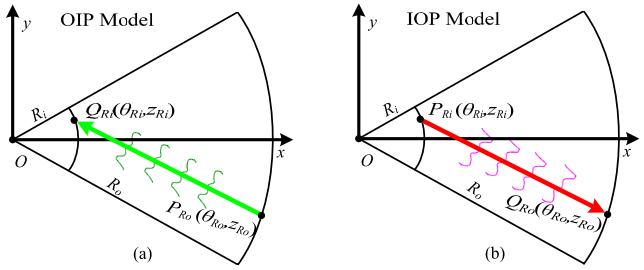

FIGURE 2. The schematic diagram of cylindrical diffraction with top-view [31]. (a) OIP Model; (b) IOP Model.

In order to specify these problems, we choose two plaintexts "Lion", and "Saturn" (Fig. 1(a), 256 × 256 pixels) as the input plaintexts. When only decryption keys (i.e. $P_0(u, v)$ and $P_1(x, y)$ are adopted for decryption, the information leaked results are shown in Fig. 1(b). And the cracked results by attack method [25]–[28] are depicted in Fig. 1(c)-1(f), respectively. Obviously, some information of the input plaintexts can be observed, which clearly illustrate its issue of information disclosure, and security.

B. CYLINDRICAL DIFFRACTION AND THE PROPOSAL

In 2005, and 2017, Sando *et al.* [29] and Wang *et al.* [30], [32] have implemented the fast calculation of cylindrical diffraction with fast Fourier transform, respectively, which provides significant assistance for extending to image encryption domain. Since the cylindrical diffraction have two propagation models, i.e. from outside to inside (OIP) and from inside to outside (IOP), shown in Fig. 2, suppose the OIP model is employed in encryption procedure, the IOP model must be adopted for decryption, vise verse. This novel propagation ways make the cylindrical diffraction possessing the characteristic of asymmetric. Thus cryptosystem build on it have higher security than the conventional DRPE has, which is based on propagation between several parallel planes.

In this paper, taking advantage of position multiplexing, we integrated the cylindrical diffraction technique into the PT-DIE scheme to achieve double-image cryptosystem. Suppose that there are two images to be processed, and they are defined as $f_i(x, y)$, $i = 1, 2$. $f_i(x, y)$ is modulated by a random phase mask (RPM) $R_i(x, y)$. So, we have

$$f_i^R(x, y) = f_i(x, y)R_i(x, y) \tag{4}$$

Apparently, in order to combine these two images as a whole, we should appropriate choose space position to keep the reconstructed two images non-overlapping. Fortunately, through position multiplexing technique [33], they are respectively located in the positions (a_i, b_i), $i = 1, 2$ of the same plane along the axes x and y, which can be written as

$$f^{pm}(x, y) = \sum_{i=1}^{2} f_i^R(x, y) * \delta(x - a_i, y - b_i) \tag{5}$$

Here, we adopt OIP model of cylindrical diffraction for encryption, the same goes for IOP model. So, the combined image $f^{pm}(x, y)$ is positioned at the outside cylindrical surface with the radii of R_o as input of cylindrical diffraction. After propagation a distance of d_1 in OIP model with the wavelength λ of the illuminating light, the wave front arrives at the intermediate surface and executes the nonlinear operation of phase-truncation, the encoded image can be expressed as follow:

$$\begin{aligned} u_{R_i}(\theta_{R_i}, z_{R_i}) &= CyD_{OIP}[f^{pm}(\theta_{R_o}, z_{R_o})] \\ g_0(\theta_{R_i}, z_{R_i}) &= Tr[u_{R_i}(\theta_{R_i}, z_{R_i})] \end{aligned} \tag{6}$$

where (θ_{R_o}, z_{R_o}) and (θ_{R_i}, z_{R_i}) are the coordinate of object and intermediate surfaces or the outside and inside cylindrical surface, respectively. And θ_{R_o}, and θ_{R_i} are in the interval of $[-\pi, \pi]$; z_{R_o} and z_{R_i} are in range of $-\frac{H}{2}$ to $\frac{H}{2}$ on the basis of the height of the cylindrical surface, H. $u_{R_i}(\theta_{R_i}, z_{R_i})$ is the distribution of inside cylindrical surface. $f^{pm}(\theta_{R_o}, z_{R_o})$ is the representation of cylindrical coordinate for $f^{pm}(x, y)$, and also is the distribution of outside cylindrical surface.

CyD_{OIP} is the OIP propagation of cylindrical diffraction, and can be mathematically calculated as

$$\begin{aligned} &CyD_{OIP}(u_{R_o}(\theta_{R_o}, z_{R_o})) \\ &= C \int\int_s u_{R_o}(\theta_{R_o}, z_{R_o}) \\ &\quad \cdot \frac{\exp(i \cdot k \cdot d_{P_{R_o}Q_{R_i}}) \cdot \cos(\alpha)}{d^2_{P_{R_o}Q_{R_i}}} d\theta_{R_o} dz_{R_o} \\ &\cos(\alpha) = [R_i - R_o \cos(\theta_{R_i} - \theta_{R_o})] \\ &\quad d_{P_{R_o}Q_{R_i}} \\ &\quad = [R_o^2 + R_i^2 - 2 \cdot R_o \cdot R_i \cdot \cos(\theta_{R_o} - \theta_{R_i}) + (z_{R_o} - z_{R_i})^2]^{\frac{1}{2}} \end{aligned} \tag{7}$$

where s, C, k, I, and λ denote the object surface, a constant, the wavenumber of the incident light, the imaginary unit, and the wavelength of the illuminating light, respectively; And $k = 2\pi/\lambda$. The $d_{P_{R_o}Q_{R_i}}$ is the distance between two points of $P_{R_o}(\theta_{R_o}, z_{R_o})$ and $Q_{R_i}(\theta_{R_i}, z_{R_i})$, as shown in Fig. 2(a), on the object and intermediate surfaces or outside and inside cylindrical surface, respectively.

Since twice direct cylindrical diffraction will lead to sampling problem of too big difference of sampling pitches, and it is impracticable [30], [32], only once cylindrical diffraction is adopted here to solve this issue. Whereafter, $g_0(\theta_{R_i}, z_{R_i})$ combines with another random phase key, $R_3(\theta_{R_i}, z_{R_i})$, and the combined result Fourier-transforms followed by phase-truncation. Thus, the final cyphertext $E(u, v)$ can be achieved as:

$$E(u, v) = Tr\{FT[g_0(\theta_{R_i}, z_{R_i}) \cdot R_3(\theta_{R_i}, z_{R_i})]\} \tag{8}$$

It can be inferred that $E(u, v)$ is a real-valued function and thus can be more convenient to record and transmit.

In the meantime, two decryption keys, i.e. private keys, $P_0(\theta_{R_i}, z_{R_i})$ and $P_1(u, v)$ are produced accompanied with encryption process.

$$\begin{aligned} P_0(\theta_{R_i}, z_{R_i}) &= Re\{CyD_{OIP}[f_t(\theta_{R_o}, z_{R_o})]\} \\ P_1(u, v) &= Re\{FT[g_0(\theta_{R_i}, z_{R_i}) \cdot R_3(\theta_{R_i}, z_{R_i})]\} \end{aligned} \tag{9}$$

For decryption, we first recover $g_0(\theta_{R_i}, z_{R_i})$ with the decryption keys $P_1(u, v)$, the process of which is similar to the decryption of PT-DIE scheme, and can be obtained by:

$$g_0(\theta_{R_i}, z_{R_i}) = IFT[E(u, v) \cdot P_1(u, v)] \cdot R_3^*(u, v) \tag{10}$$

where the superscript $*$ is the operator of conjugation.

Then, $g_0(\theta_{R_i}, z_{R_i})$ is modulated by another private key $P_0(\theta_{R_i}, z_{R_i})$. The complex amplitude distribution, $f_t(\theta_{R_o}, z_{R_o})$, is obtained after a IOP model propagation of inverse cylindrical diffraction with the wavelength λ of the illuminating light, can be expressed as:

$$f_t(\theta_{R_o}, z_{R_o}) = CyD_{IOP}[g_0(\theta_{R_i}, z_{R_i}) \cdot P_0(\theta_{R_i}, z_{R_i})] \tag{11}$$

where CyD_{IOP} represents the inverse process of CyD_{OIP} and can be calculated as the Rayleigh-Sommerfeld integral formulas.

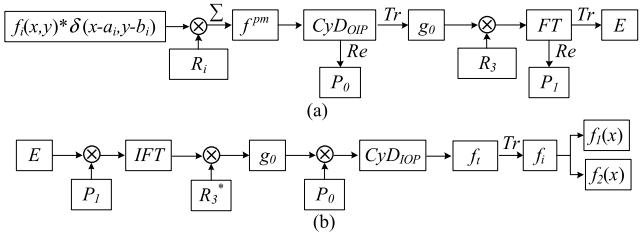

FIGURE 3. Flowcharts of encryption process (a) and decryption process (b).

$$\begin{aligned} &CyD_{IOP}(u_{R_i}(\theta_{R_i}, z_{R_i})) \\ &= C \int\int_s u_{R_i}(\theta_{R_i}, z_{R_i}) \cdot \frac{\exp(i \cdot k \cdot d_{P_{R_i}Q_{R_o}})}{d_{P_{R_i}Q_{R_o}}} d\theta_{R_i} dz_{R_i} \end{aligned} \tag{12}$$

where $u_{R_i}(\theta_{R_i}, z_{R_i})$ denotes $g_0(\theta_{R_i}, z_{R_i}) \cdot P_0(\theta_{R_i}, z_{R_i})$, $d_{P_{R_i}Q_{R_o}} = d_{P_{R_o}Q_{R_i}}$, $k = 2\pi/\lambda$. The $d_{P_{R_i}Q_{R_o}}$ is the distance between two points of $P_{R_i}(\theta_{R_i}, z_{R_i})$ and $Q_{R_o}(\theta_{R_o}, z_{R_o})$, as shown in Fig. 2(b), on the intermediate and object surfaces or inside and outside cylindrical surface, respectively. Moreover, since the cylindrical diffraction model in encryption process is OIP, the inverse propagation of it is IOP model here under conditions of (R_i, R_o, H, λ), vise verse.

It is seen that due to position multiplexing, the information from different input plaintexts are independent from each other. Then $f^{pm}(x, y)$ is considered as the object image of the cylindrical diffraction, followed by the phase-truncation operator. The details of this process is described as follows.

In the last, the spectrum of inverse cylindrical diffraction is operated with the phase-truncation, and the output can be obtained as:

$$\begin{aligned} f^{pm}(x, y) &= Tr[f_t(\theta_{R_o}, z_{R_o})] \\ &= \sum_{i=1}^{2} f_i(x, y) * \delta(x - a_i, y - b_i) \end{aligned} \tag{13}$$

Clearly, two original images ($f_1(x, y)$, and $f_2(x, y)$) can be easily extracted from the output. In order to illustrate the encryption and the decryption procedure, the flowcharts for them are shown in Fig. 3(a) and 3(b), respectively.

C. PERFORMANCE ANALYSIS

From the aforementioned description of cryptosystem, although the position multiplexing technique, and cylindrical diffraction are deployed in the encryption procedures, they only change the composing form of input image from individual treatment to integrated operation, and the mode of propagation from parallel planes to cylindrical surface. Obviously, no linear component is brought in. Thus, the nonlinear characteristic is still kept in our proposed scheme. Meanwhile, since the decryption keys ($P_0(\theta_{R_i}, z_{R_i})$ and $P_1(u, v)$) is related to the input double-image or multi-image, the proposed method is free of known-plaintext attack, and chosen-plaintext attack in theoretically. In addition, since the inverse propagation of OIP model is IOP

model in optical setup, and the diffraction calculation of propagation of OIP model is also different from that of the reversed direction, i.e. IOP model, the cylindrical diffraction is asymmetric, and thus is free of the phase-retrieval attack, and information disclosure. Hence the proposed algorithm can also resist the phase retrieval algorithm-based attacks, covering Deng's attack [25], a generalized phase retrieval algorithm (GPRA) attack [27], a special attack [28], and the simple public-key attack [26], even information leakage analyzed as follows.

If only the constraints or preconditions are broken, the phase retrieval algorithm-based attacks [25], [27], [28], and the simple public-key attack [26] can be avoided. For Deng's attack, using the cyphertext $E(u, v)$, R_3 and the encryption key $g_0(\theta_{R_i}, z_{R_i})$, the plaintexts can be approximately estimated by operating iterative transform. But, on account of asymmetric cylindrical diffraction, the positive image and the phase mask blend together, making the preconditions ($FT[f_2(x, y)] * FT(R_2) \approx FT(R_2)$ and $FT[f_1(x, y)] * FT(R_1) \approx FT(R_1)$) invalid. That is, $CyD_{OIP}[f_2(x, y)] * CyD_{OIP}(R_2) \neq CyD_{OIP}(R_2)$ and $CyD_{OIP}[f_1(x, y)] * CyD_{OIP}(R_1) \neq CyD_{OIP}(R_1)$. Thus, original double-image will not be obtained correctly. For the simple public-key attack, it need two error-functions to approximate 1. Similar to the invalid reasons of Deng's attack, the two error-functions cannot converge to 1, causing the attacked results incorrectly.

For the GPRA attack or the special attack, the main process is modified as our proposed method and calculated as:

(1) Arbitrarily set two matrices $f_i'(x, y), i = 1, 2$ and position parameters $(a_i', b_i'), i = 1, 2$ as the estimations of the original plaintexts and position parameters. Then, their integration is given by

$$f'(x, y) = \sum_{i=1}^{2} f_i'(x, y) R_i(x, y) * \delta(x - a_i', y - b_i') \quad (14)$$

(2) A cylindrical diffraction and the phase truncation are performed, the results are given by

$$\begin{aligned} E_k &= Tr\{FT[Tr\{CyD_{OIP}[f'(x, y)]\}R_3]\} \\ P_{1k} &= Re\{FT[Tr\{CyD_{OIP}[f'(x, y)]\}R_3]\} \end{aligned} \quad (15)$$

(3) E_k is substituted with the cyphertext E. Then an inverse cylindrical diffraction and phase truncation are executed, the estimated plaintexts $f_i'(x, y), i = 1, 2$ are obtained by

$$f_i' = Tr\{CyD_{IOP}[IFT(E \cdot P_{1k}) \cdot R_3^*]\} \quad (16)$$

(4) Repeated steps 1-3 until the iteration number reaches a preset threshold value.

From these iterative phase retrieval procedures, we can see that the constraints are the public keys $(R_i, i = 1, 2, 3)$, the cyphertext $E(u, v)$, and the parameters (R_i, R_o, H, λ) of cylindrical diffraction. Because the OIP model and IOP model is not symmetric, and the deduction process of them is also different plus their parameters (R_i, R_o, H, λ) also unpublicized, the constraints (i.e. $E(u, v)$, and (R_i, R_o, H, λ)) will be broken and original images will not be cracked correctly with iterative transforms.

For the issue of information disclosure of the conventional PT-DIE scheme as described in section Section II-A, when both decryption keys are directly used to decode, the primary information of the input plaintexts can be clearly observed, as shown in Fig. 1(b). In order to theoretical discuss whether our proposed scheme can resist the information disclosure, we firstly modify the phase key $P_0(u, v)$ since $R_3^*(\theta_{R_i}, z_{R_i})$ is essential for decryption, and expressed as

$$P_0'(\theta_{R_i}, z_{R_i}) = P_0(\theta_{R_i}, z_{R_i}) \cdot R_3^*(\theta_{R_i}, z_{R_i}) \quad (17)$$

where $R_3^*(\theta_{R_i}, z_{R_i})$ is the complex conjugate of $R_3(\theta_{R_i}, z_{R_i})$. Then the phase modulation executes with $P_0(\theta_{R_i}, z_{R_i})$ and $P_1(u, v)$ for decryption, and the result of information disclosure, $ID(x, y)$, can be calculated as

$$\begin{aligned} &ID(x, y) \\ &= [E(x, y) \cdot P_1(u, v)] \cdot CyD_{IOP}[P_0'(\theta_{R_i}, z_{R_i})] \\ &= CyD_{IOP}\{CyD_{OIP}[E(x, y) \cdot P_1(u, v)]\} \\ &\quad \cdot CyD_{IOP}[P_0'(\theta_{R_i}, z_{R_i})] \\ &= CyD_{IOP}\{CyD_{OIP}[E(x, y) \cdot P_1(u, v)] \cdot P_0'(\theta_{R_i}, z_{R_i})\} \\ &= CyD_{IOP}\{CyD_{OIP}[E(x, y) \cdot P_1(u, v)] \\ &\quad \cdot P_0(\theta_{R_i}, z_{R_i}) \cdot R_3^*(\theta_{R_i}, z_{R_i})\} \end{aligned} \quad (18)$$

Suppose $CyD_{OIP}[E(x, y) \cdot P_1(u, v)] = IFT[E(u, v) \cdot P_1(u, v)]$

$$\begin{aligned} &ID(x, y) \\ &= CyD_{IOP}[g_0(\theta_{R_i}, z_{R_i}) \cdot R_3(\theta_{R_i}, z_{R_i}) \cdot P_0(\theta_{R_i}, z_{R_i}) \\ &\quad \cdot R_3^*(\theta_{R_i}, z_{R_i})] \\ &= CyD_{IOP}[g_0(\theta_{R_i}, z_{R_i}) \cdot P_0(\theta_{R_i}, z_{R_i})] \\ &= f_t(\theta_{R_o}, z_{R_o}) = f_i(x, y) R_i(x, y) \quad i = 1, 2 \end{aligned} \quad (19)$$

But, unfortunately, what we have assumed here were not true, that is $CyD_{OIP}[E(x, y) \cdot P_1(u, v)] \neq IFT[E(u, v) \cdot P_1(u, v)]$. Thus, $ID(x, y)$ cannot be deduced to the input plaintext. That means the proposed scheme can resist the information disclosure.

The conclusion can be drawn that because of using position multiplexing and phase-truncation in cylindrical diffraction domain, our proposed algorithm holds the nonlinear characteristic, and have higher security than the conventional PT-DIE cryptosystem has.

D. OPTICAL REALIZATION

The proposed cryptosystem is also suggested for optical verification due to its simple optical implementation. A possible implementation displays in Fig. 4. $f_t(\theta_{R_o}, z_{R_o})$, and R_3 represent double-image modulated by two random phase keys (R_1, and R_2), and random phase key, respectively. The input object $f_t(\theta_{R_o}, z_{R_o})$ locates at the source surface with radii of R_o and propagates to the intermediate surface with radius of R_i, on which the distribution is $u_{R_i}(\theta_{R_i}, z_{R_i})$. Through the operations of phase-truncation and phase-reservation, the encrypted image is captured by CCD.

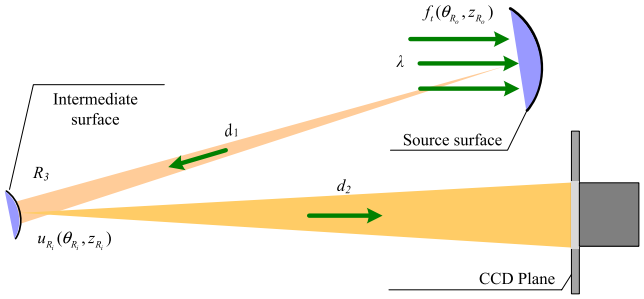

FIGURE 4. A possible implementation of the proposed cryptosystem.

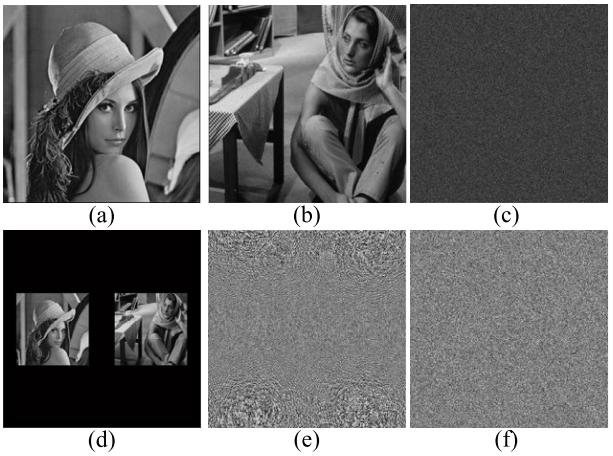

FIGURE 5. (a) Lena; (b) Barbara; (c) the cyphertext; (d) the correct decrypted result; the phase part of decryption keys (e) P_0, and (f) P_1.

Since the decryption is the inverse process of encryption, a possible implementation of decryption is in the reversed order of encryption procedures. Due to the current resource limitation in our laboratory, some numerical simulations are made to test the feasibility and effectiveness of our proposed algorithm.

III. NUMERICAL SIMULATION

A. ENCRYPTION AND DECRYPTION RESULTS

Numerical experiments are conducted to verify our proposed cryptosystem with Matlab 2017(a) on a 64-bit computer. The parameters (R_i, R_o, H, λ) of cylindrical diffraction are set as 10mm, 100 mm, 64 mm, and 96 um, respectively, and can be also employed as the keys of cylindrical diffraction. Two original images, "Lena" (256 × 256 pixel) and "Barbara" (256 × 256 pixel), which are shown in Fig. 5(a) and 5(b), can be used as the object images for double-image encryption. For guaranteeing the retrieved two images without being superimposed, the two images are located in the centered and zero-padded images (700 × 700 pixels) as the input plaintexts, and the two position parameters (a_1, b_1) and (a_2, b_2) are set as $(-175, 0)$, and $(175, 0)$, respectively. Figure 5(c) and 5(d) represent the encryption result, and the correct decrypted image. From them, it can be seen that the encryption image shows good noise-like property, and the decrypted images shows good retrieved quality. The two decryption keys produced in the encryption procedures,

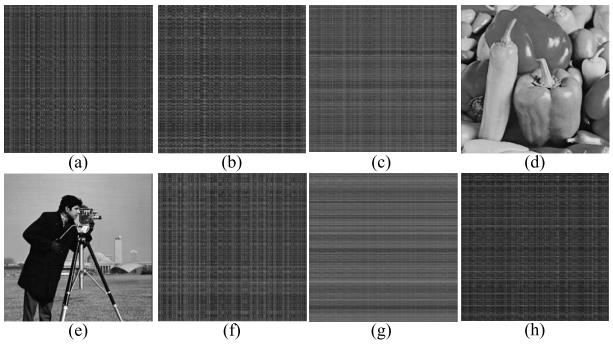

FIGURE 6. Decrypted results with (a) no keys; (b) arbitrarily chosen decryption keys; (c) the encryption keys; two fake plain images (d) Peppers; and (e) Cameraman; (f) decrypted results with the phase keys generated from (d), and (e); (g) the correct key P_0 while P_1 is wrong; (h) the correct key P_1 while P_0 is wrong.

and adopted for the correct decryption are displayed in Fig. 5(e), and 5(f).

To evaluate the reliability of this method, the Correlation Coefficient (CC) value between the plaintext, f, and the decrypted image, f', is adopted and can be calculated by the following equation:

$$CC = \left| \frac{cov(f, f')}{\sigma_f \times \sigma_{f'}} \right| \tag{20}$$

where cov and σ denote cross-covariance, and standard deviation, respectively. Here, the coordinates (x,y) are omitted for the sake of brevity. The CC values between the input plaintext, and the Fig. 5(d) is one, which means the decryption process is the lossless inverse of the encryption process.

B. CONVENTIONAL ATTACKS AND THE PHASE RETRIEVAL ALGORITHM-BASED ATTACK

In this section, same attacks are executed with different keys. The result of brute force attack using no decryption keys is shown in Fig. 6(a). Figure 6(b) displays the result of arbitrarily chosen decryption keys. The attack result with the public keys is represented in Fig. 6(c). Figures 6(d)-6(e), with the names of "Peppers" and "Cameraman", are the two fake plain images that employed to produce decryption keys. As can be seen from Fig. 6(f), the recovered image offers no valuable information when the fake keys are used for decryption. Attacks with a part of public keys are also shown in Fig. 6(g) and 6(h). Figure 6(g) is the decryption result using the correct key P_0 while P_1 is wrong. The attack result, which realized using the correct key P_1 while P_0 is wrong, is demonstrated in Fig. 6(h). In addition, the CC values corresponding to Fig. 6(a)-6(c) and 6(f)-6(h) are 0.0096, 0.0112, 0.0204, 0.0153, 0.0219 and 0.0038, respectively. These results verify that any attempt at the decryption of cyphertext without correctly decryption keys will fail.

Figure 7 displays the attack results using the phase retrieval algorithm-based attacks, including Deng's attack [25], GPRA attack [27], and the special attack [28], and the simple public-key attack [26]. The original double-image are the combination of "Lion", and "Saturn", shown in Fig. 1(a).

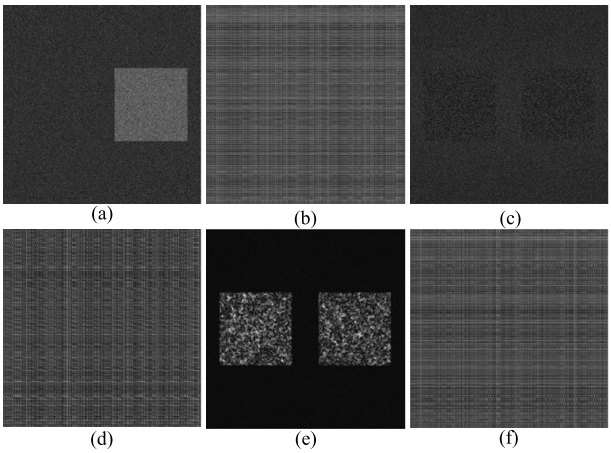

FIGURE 7. The results of (a) Deng's attack [25]; (b) simple public-key attack [26]; GPRA [27] attack (c) without diffraction parameters; (d) with correct diffraction parameters; Special attack [28] (e) without diffraction parameters; (f) with correct diffraction parameters.

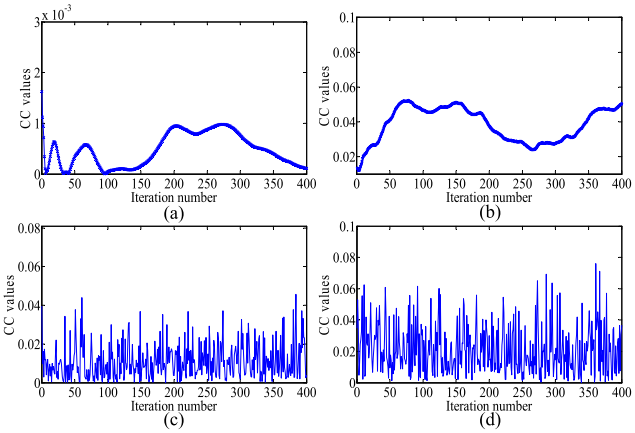

FIGURE 8. Relation between iteration times and the CC values (a) GPRA without diffraction parameters; (b) special attack without diffraction parameters; (c) GPRA with correct diffraction parameters; (d) special attack with correct diffraction parameters.

Deng's attack, and the simple public-key attack do not need any knowledge of cryptosystem to be crack except for three public keys. Thus, theirs attacked results are shown in Fig. 7(a) and 7(b), respectively. Supposing the intruder has no knowledge of proposed cryptosystem, the decrypted results of GPRA, and the special attack are displayed in Fig. 7(c) and 7(e). Therewith the adversary may improve the attack of GPRA, and the special attack with the correct cylindrical diffraction process. The simulation results under this condition are represented in Fig. 7(d) and 7(f). These results illustrate that the phase retrieval-based attack algorithm is inefficient for the proposed improvement cryptosystem. The CC values between decrypted plaintexts shown in Fig. 7(a)-7(f) and original one are 0.2595, 0.0018, 0.0016, 0.0457, 0.0521, and 0.0760, respectively. The relationship between the iteration number and the CC values [between plaintext and its estimate] are displayed in Figs. 8(a) and 8(b) without the knowledge of cylindrical diffraction for GPAR, and the special attack, respectively. Figures 8(c) and 8(d)

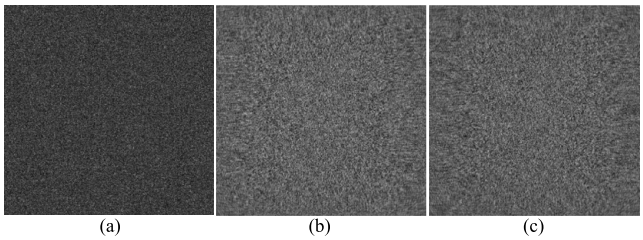

FIGURE 9. Recovered results with disclosure of (a) P_0, (b) P_0 plus E, (c) P_0 plus P_1.

show the corresponding relation between iteration number and the CC values under the cylindrical diffraction condition. They demonstrate that the plaintext's information cannot be recovered.

In conclusion the designed cryptosystem has the ability of invalidating the phase retrieval-based attack no matter if the attacker has the prior knowledge of cylindrical diffraction.

C. THE ANALYSIS OF INFORMATION DISCLOSURE

As reported in reference [18], the information disclosure is defined as when lacking any one of the cyphertext or decryption keys in the decryption procedure, some information about the input plaintext can be clearly observed. While full-failed decryption means no information of the input plaintexts is recovered from the decrypted results. This means it is free of information disclosure. Here we carried out an experiment to test whether the proposed scheme can resist the issue of information disclosure as the same as the theoretical analysis. In our proposed algorithm, the decryption keys (P_0, and P_1) for double-image are hidden in the cylindrical diffraction with the cyphertext of E. When only P_0, P_0 plus E, P_0 plus P_1 for double-image (''Lena'' and ''Barbara''), the recovered results are displayed in Fig. 9(a), 9(b), and 9(c), respectively. It can be observed that information of the original double-image is not divulged at all, which is consistent with theoretical analysis. Therefore, the risk of information disclosure has completely been eliminated from our proposed scheme.

D. KEY SENSITIVITY ANALYSIS

Generally, the sensitivity of the encryption parameters should be considered to address whether the cryptosystem is stable. Compared with the conventional PT-IDE cryptosystem, our proposed method mainly introduces four parameters, i.e. (R_i, R_o, H, λ) of cylindrical diffraction. Thus, it will be necessary to study the sensitivity of the decrypted results to the four parameters. Figure 10(a) shows the decrypted results with the outer cylinder Ro under a slight deviation ΔR_o while other keys remain unchanged. Obviously, the decrypted results cannot be correctly recovered. In the same ways, varying the parameters of (R_i, H, λ), the results are shown in Fig. 10(b)- 10(d). Meanwhile, the CC values between the plaintext, and the Fig. 10(a)-10(d) are 0.0202, 0.0122, 0.0125, and 0.0022, respectively. Furthermore, the corresponding CC values between the original and the decrypted results, as the function of the ΔR_o, ΔR_i, ΔH and $\Delta\lambda$,

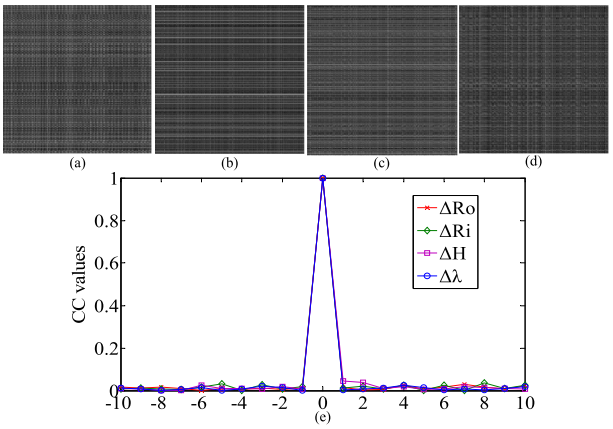

FIGURE 10. The decrypted double-image with incorrect keys: (a) $\Delta R_o = 0.001$ mm; (b) $\Delta R_i = 0.001$ mm; (c) $\Delta H = 0.0001$ mm; (d) $\Delta\lambda = 0.001$ um; (e) The CC values varies with (ΔR_o (mm/1000), ΔR_i(mm/1000), ΔH(mm/10000), $\Delta\lambda$(um/1000)).

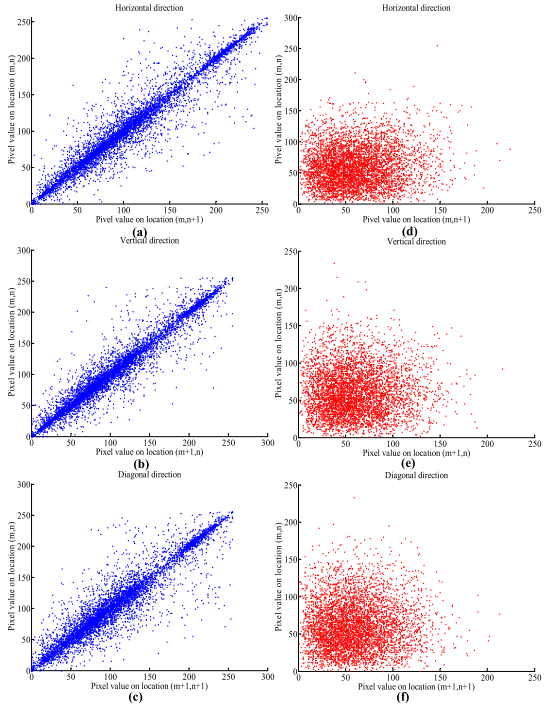

FIGURE 11. Histograms of (a) Lena; (b) Barbara; (c) the input double-image; (d) the encrypted image; (e) the encrypted images from the SIPI database [34].

are shown in Fig. 10(e). The above results fully illustrate that when using an arbitrarily chosen parameters to recover the plaintext, it will fail.

E. OTHER ATTACKS

In this section, we first consider the statistical analysis of the plaintext images and the cyphertext image. Figs. 11(a)-11(c) show the histograms of two plaintext images, the input double-image, and the corresponding histogram of cyphertext image, respectively. Subsequently, we further adopt another 50 images from the USC Signal

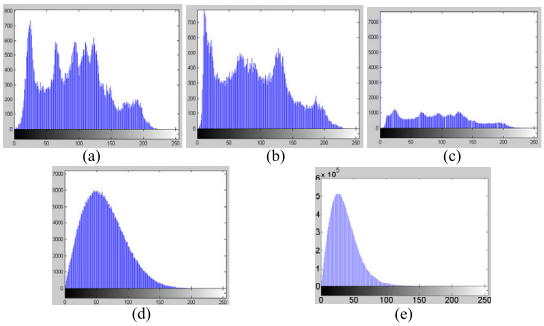

FIGURE 12. Correlation of two adjacent pixels before (a)-(c) and after (d)-(f) encryption in the horizontal, vertical, and diagonal directions, respectively.

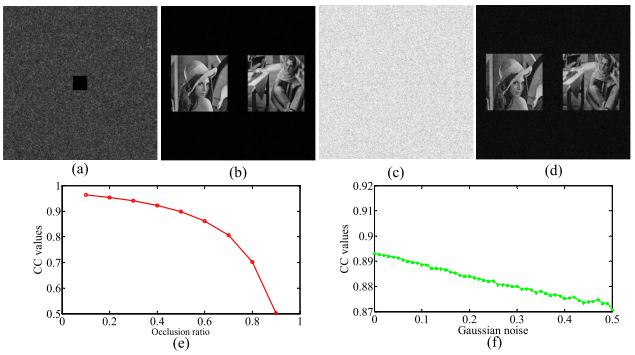

FIGURE 13. The occlusion encrypted image; (b) the corresponding retrieved image from (a); (c) Gaussian-noised encrypted image with variance value 0.1; (d) corresponding decrypted image from (c); the CC value curves from (e) the occlusion attack; (f) the Gaussian noise attack.

and Image Processing Institute database (SIPI dataset) [34] for encryption, and display the corresponding histogram of their cyphertext in Fig. 11(e). It is observed that the histogram of cyphertext image has similar distribution, and is evidently different from that of plaintext images.

Then, six thousand pixel pairs from the selected 50 plaintext images from the SIPI database [34] (in the horizontal, vertical, and diagonal directions) are randomly chosen to test the correlation of two adjacent pixels. Figs. 12 (a)-(c) and 12 (d)-(f) display correlations of adjacent pixels before and after encryption in the horizontal, vertical, and diagonal directions, respectively. Obviously, the correlations of adjacent pixels of the cyphertext are remarkable reduced compared with those of original plaintexts in all the three directions. The above results and analysis demonstrate that no valuable information can be obtained from the statistical analysis of the histograms and correlations.

Next, the robustness of the cryptosystem against noise and occlusion attacks on the encrypted results also should be checked. The occluded encrypted images with 64×64 pixels, and its corresponding recovered image are displayed in Fig. 13(a) and 13(b). For noise attack, the Gaussian-noised encrypted image with variance value 0.1 is depicted in Fig. 13(c) and the corresponding recovered image is shown in Fig. 13(d). The CC values corresponding to Fig. 13(b) and Fig. 13(d) are 0.9709, and 0.9479, respectively. It can be

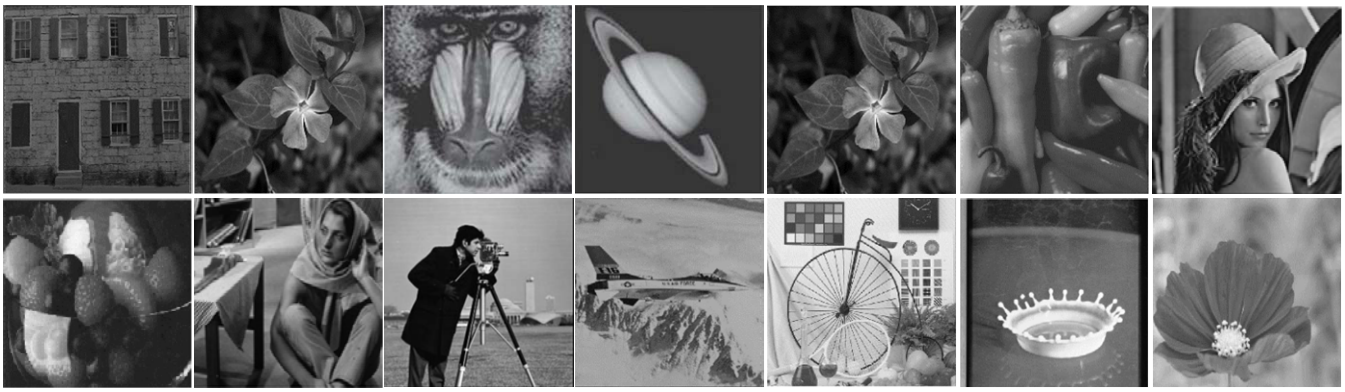

FIGURE 14. The adopted fourteen images.

TABLE 1. The executing times of the encryption process, and the corresponding CC values between the decrypted results and the input multi-image.

Method	Parameter	two images	four images	eight images	twelve images	thirteen images	fourteen images
Proposed	Time	0.1272	0.1374	0.1431	0.1477	0.1497	0.1531
	CC	1.0000	1.0000	1.0000	1.0000	0.9784	0.9404
[34]	Time	0.1465	0.2375	0.4417	0.6974	0.9551	1.2980
	CC	1.0000	1.0000	1.0000	0.9839	0.1840	0.1479

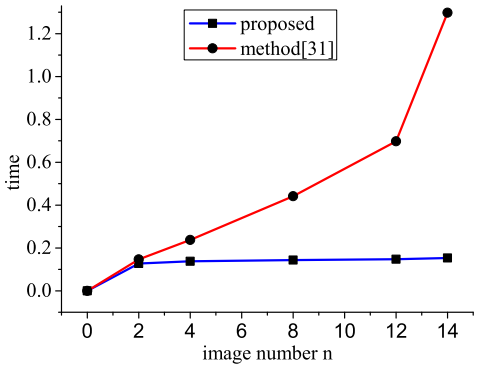

FIGURE 15. The encryption time of different numbers of images.

gained that the decrypted images exhibit most information of the input image. Next, the CC values of the occlusion attack and Gaussian-noise attack in the range [0.1, 0.9] and [0, 0.5] are shown in Fig. 13(e) and 13(f), respectively. From these figures, they indicate that the CC value decreases with an increase in occlusion size or Gaussian noise. The above experimental results manifest that our proposed algorithm can resist the occlusion and Gaussian-noise attack.

F. SYSTEM EXPANDABILITY

The proposed scheme can extend to encode more images by appropriate choosing space position with position multiplexing technique. In essence, the proposed scheme can encode infinite images, but the resolution of integrated images may increase by an integer factor. Hence, 2, 4, 8, 12, 13, and 14 different images with 256×256 pixels, shown in Fig. 14, are executed with the proposed scheme and the method [31], respectively. Here, the time spent in the process of multi-image with different numbers, and the corresponding average CC values are counted.

The results are demonstrated in Table 1 and Fig. 15. Clearly, the encryption time of the proposed scheme slightly increase with the increment of images, but the comparative method [31] remarkably augments. Meanwhile, the quality of method [31] begin to degrade significantly when the number of encrypted images reaches 12. However, most information of the decrypted images are also retained, and theirs visual quality almost no change.

IV. CONCLUSION

To conclude, we have developed an scheme for double-image cryptosystem. By aid of position multiplexing, two primary images are compacted into a single gray image, which are further encoded into a real-valued amplitude cyphertext by cylindrical diffraction, accompanied by two phase decryption keys. For decryption, the double-plaintext can be obtained through inverse cylindrical diffraction if all parameters are correct. Compared with the conventional PT-IDE methods, our proposed scheme can overcome the information disclosure issue, and increases the system security. Meanwhile, it is also demonstrated to be robust to the various attacks, especially the phase-retrieval-based attacks, for the introduction of cylindrical diffraction strategy, which possesses the nonlinear characteristic and asymmetric structure. Furthermore, the extended multi-image cryptosystem of our proposed scheme maintain the original cylindrical-diffraction structure except for the object surface composition. As a result, the encryption procedure of multi-image does not add extra computing time, and the quality of decryption is also guaranteed. Simulations results demonstrate that the proposed algorithm is feasible and effective for double-image or multi-image encryption. In the future, we will apply this scheme to some applications, such as authentication, QR code, anti-counterfeiting and other fields.

REFERENCES

[1] O. S. Faragallah, M. A. Alzain, and H. S. El-Sayed, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2018.
[2] R. Kumar, J. T. Sheridan, and B. Bhaduri, "Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm," *Opt. Laser Technol.*, vol. 107, pp. 353–360, Nov. 2018.
[3] Y. Luo, X. Ouyang, J.-X. Liu, and L.-C. Cao, "An image encryption method based on elliptic curve ElGamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
[4] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double-image encryption scheme based on amplitude-phase encoding and discrete complex random transformation," *IEEE Access*, vol. 6, pp. 77740–77753, 2018.
[5] S. Liansheng, D. Cong, Z. Xiao, T. Ailing, and A. Anand, "Double-image encryption based on interference and logistic map under the framework of double random phase encoding," *Opt. Lasers Eng.*, vol. 122, pp. 113–122, Nov. 2019.
[6] S. Liansheng, W. Jiahao, T. Ailing, and A. Asundi, "Optical image hiding under framework of computational ghost imaging based on an expansion strategy," *Opt. Express*, vol. 27, no. 5, pp. 7213–7225, 2019.
[7] S. Liansheng, D. Cong, X. Minjie, T. Ailing, and A. Anand, "Information encryption based on the customized data container under the framework of computational ghost imaging," *Opt. Express*, vol. 27, no. 12, pp. 16493–16506, 2019.
[8] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.
[9] Y. Wang, C. Quan, and C. J. Tay, "Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain," *Opt. Commun.*, vol. 330, no. 1, pp. 91–98, Nov. 2014.
[10] 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.
[11] 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.
[12] L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Opt. Express*, vol. 14, no. 19, pp. 8552–8560, 2006.
[13] 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, Apr. 2006.
[14] 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.
[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] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, 2010.
[17] 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, 2012.
[18] X. Wang and D. Zhao, "Double images encryption method with resistance against the specific attack based on an asymmetric algorithm," *Opt. Express*, vol. 20, no. 11, pp. 11994–12003, 2012.
[19] M. R. Abuturab, "An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain," *Opt. Lasers Eng.*, vol. 58, no. 4, pp. 39–47, 2014.
[20] L. Sui, K. Duan, J. Liang, Z. Zhang, and H. Meng, "Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain," *Opt. Lasers Eng.*, vol. 62, pp. 139–152, Nov. 2014.
[21] W. Liu, Z. Liu, and S. Liu, "Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang-Gu algorithm," *Opt. Lett.*, vol. 38, no. 10, pp. 1651–1653, 2013.
[22] X. Ding, X. Deng, K. Song, and G. Chen, "Security improvement for asymmetric cryptosystem based on spherical wave illumination," *Appl. Opt.*, vol. 52, no. 3, pp. 467–473, 2013.
[23] X. Wang, D. Zhao, and Y. Chen, "Double-image encryption without information disclosure using phase-truncation Fourier transforms and a random amplitude mask," *Appl. Opt.*, vol. 53, no. 23, pp. 5100–5108, 2014.
[24] Y. Wang, C. Quan, and C. J. Tay, "Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask," *Opt. Commun.*, vol. 344, pp. 147–155, 2015.
[25] X. Deng, "A hybrid attack on 'double images encryption method with resistance against the specific attack based on an asymmetric algorithm,"' *Opt. Commun.*, vol. 317, pp. 7–12, 2014.
[26] X. Ding, G. Yang, and D. He, "A simple public-key attack on phase-truncation-based double-images encryption system," *Opt. Commun.*, vol. 346, pp. 141–148, 2015.
[27] C. Zhang, W. He, Z. Cai, and X. Peng, "Generalized amplitude-phase retrieval algorithm attack on 'double images encryption method with resistance against the special attack based on an asymmetric algorithm,"' in proc of *Proc. SPIE*, vol. 9970, Sep. 2016, Art. no. 997018.
[28] 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, 2018.
[29] Y. Sando, M. Itoh, and T. Yatagai, "Fast calculation method for cylindrical computer-generated holograms," *Opt. Express*, vol. 13, no. 5, pp. 1418–1423, 2005.
[30] J. Wang, Q. Wang, and Y. Hu, "Fast diffraction calculation of cylindrical computer generated hologram based on outside-in propagation model," *Opt. Commun.*, vol. 403, pp. 296–303, 2017.
[31] J. Wang, Y. Hu, and Q. Wang, "Asymmetric color image cryptosystem using detour cylindrical-diffraction and phase reservation & truncation," *IEEE Access*, vol. 6, pp. 53976–53983, 2018.
[32] J. Wang, Q. Wang, and Y. Hu, "Unified and accurate diffraction calculation between two concentric cylindrical surfaces," *J. Opt. Soc. Amer. A.*, vol. 35, no. 1, pp. A45–A52, 2018.
[33] J. F. Barrera and R. Torroba, "One step multiplexing optical encryption," *Opt. Commun.*, vol. 283, no. 7, pp. 1268–1272, 2010.
[34] *The USC Signal and Image Processing Institute Database*. Accessed: Nov. 1, 2019. [Online]. Available: http://sipi.usc.edu/database/