IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 11, 2019, accepted May 17, 2019, date of publication May 20, 2019, date of current version June 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2917994

Asymmetric Cryptosystem Using Improved Equal Modulus Decomposition in Cylindrical Diffraction Domain

JUN WANG[1,2], XUDONG CHEN[2], JIANQING ZENG[2], QIONG-HUA WANG[1], AND YUHEN HU[3], (Fellow, IEEE)

[1]School of Instrumentation and Optoelectronic Engineering, Beihang University, Beijing 100191, China
[2]School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China
[3]Department of Electrical & Computer Engineering, University of Wisconsin - Madison, Madison, WI 53706, USA

Corresponding author: Qiong-Hua Wang (qionghua@buaa.edu.cn)

This work was supported by the National Key Research and Development Program of China under Grant 2017YFB1002900.

ABSTRACT We present a simple and efficient asymmetric cryptosystem using an improved equal modulus decomposition (EMD) in the cylindrical diffraction domain. Being different from a cryptosystem based on the conventional EMD, whose outputs are complex-valued, in the planer diffraction domain, our proposed cryptosystem uses the improved EMD and the cylindrical diffraction. Therefore, the proposed system achieves high robustness against the special attack based on iterative retrieval algorithms. Moreover, it has a merit of real-valued outputs due to the improved EMD. In addition, our proposed asymmetric cryptosystem achieves comparative advantages on encryption time, optical decryption complexity, and the data amount of storage or transmission when it is compared with the conventional EMD-based cryptosystems. The simulation results verify the validity of the proposed system.

INDEX TERMS Optical encryption, equal modulus decomposition, cylindrical diffraction.

I. INTRODUCTION

As increasing challenges of how to efficiently and adequately protect, process, transfer, and store the mass information in modern societies, optical technologies have been widely applied in these procedures, including information securing applications, owing to the potential capability of processing information in the speed of light [1]. Since the pioneering research of the double random phase encryption (DRPE) was proposed by Refregier and Javidi [2], image encryption has become increasingly attractive as a hot issue of optical information securing. Further developments lead to DRPE being implemented in many optical schemes [3]–[14]. However, these optical cryptosystems based on DRPE are vulnerable to different types of attacks [15]–[17] due to their inherent linearity. Therefore, it is very important to develop asymmetric cryptosystems to solve these problems in the symmetric cryptosystems.

Amount of excellent works on asymmetric cryptosystems have been developed. One important scheme is using phase-truncated Fourier transforms (PTFT), which was firstly proposed by Peng [18]. Although the PTFT-based cryptosystem has some developments on the security enhancement [19]–[21], it is unfortunately vulnerable to the special attacks [22], [23], which are based on iterative Fourier transforms. The other scheme is the interference based cryptosystem, which was firstly proposed by Zhang and Wang [24]. It has been devoted great efforts to extend to binary, color or multiple images encryption [25]–[27] and to improve the security [28], [29]. Unfortunately, this scheme still suffers from the inherent problem of silhouette [30], and some silhouette-free researches [31]–[33] have been proposed, recently. Another scheme is based on the interference principle and equal modulus decomposition (EMD), which was proposed by Cai *et al.* [34]. Since the EMD based cryptosystems are still threatened by the special attack of iterative retrieval algorithms (IRA) [35], [36], security enhancements have been proposed by introducing full phase encryption technique [37], fractional Fourier domain [38], [39], cascaded EMD [40], gyrator transform [41], Fresnel domain [42], unequal modulus decomposition [43], and singular value decomposition [44]. However, in most of the enhanced methods based on EMD, the issue of complex-valued outputs of

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

EMD is ignored, which needs double space to save or transmit compared with real-valued outputs. In addition, the enhanced solutions are rather complex, which results in either more computation time in digital encryption or higher implementation cost in optical decryption. Therefore, despite significant progress, there still exists a grand challenge to develop a simple and efficient asymmetric cryptosystem with higher security of free of silhouette and IRA attack as well as comparative advantages on encryption time, optical decryption complexity, and the data amount of storage or transmission. Furthermore, the EMD based encryption has not been employed in cylindrical diffraction domain.

In this paper, a simple and efficient asymmetric cryptosystem based on the EMD in the cylindrical diffraction domain is proposed to hide an image into two real-valued masks which are one pure phase as a private key and one pure amplitude as ciphertext. As far as we known, it is the first time to encrypt image by using EMD in cylindrical diffraction domain. Being different from the cryptosystems based on conventional EMD in planer diffraction domain, an improved EMD (IEMD) and the cylindrical diffraction are employed in our proposed cryptosystem. Here, the using of cylindrical diffraction mainly contributes silhouette-free and high robustness against the special attacks based on IRAs. In addition, the proposed IEMD ensures real-valued outputs, which saves data amount of storage or transmission. Previously, we have proved the merit of high security of IRA-free using the cylindrical diffraction to replace the planer diffraction in proposed cryptosystem based on DRPE in cylindrical diffraction domain [45] and the proposed cryptosystem using detour cylindrical diffraction and compressive sensing [46]. Compared with our previous researches, this proposed cryptosystem employees only single cylindrical diffraction and is a cryptosystem with asymmetric keys. The proposed asymmetric cryptosystem also achieves comparative advantages on encryption time, optical decryption complexity, and the data amount of storage or transmission compared with the conventional EMD based cryptosystems [29], [34], [37].

II. PRINCIPLE

A. THEORETICAL ANALYSIS

The procedure for the asymmetric cryptosystem based on improved EMD in cylindrical diffraction domain can be described as follows.

Firstly, a digital image to be encrypted is denoted $I(m, n)$. It can be mapped to an intensity distribution of $I(\theta_1, z_1)$ on a cylinder. Here, (m, n) and (θ_1, z_1) denote coordinates of plaintext in Cartesian and cylindrical coordinate systems, respectively. Therefore, a function $U_2(\theta_2, z_2)$ can be constructed as

$$\begin{aligned} U_2(\theta_2, z_2) &= I\mathrm{CDT}\{U_1(\theta_1, z_1)\} \\ &= I\mathrm{CDT}\left\{\sqrt{I(\theta_1, z_1)} \times \exp\left[iR_1(\theta_1, z_1)\right]\right\}, \end{aligned} \quad (1)$$

where $R_1(\theta_1, z_1)$ denotes a random phase mask (RPM), $U_1(\theta_1, z_1)$ and $U_2(\theta_2, z_2)$ are the input and output of ICDT,

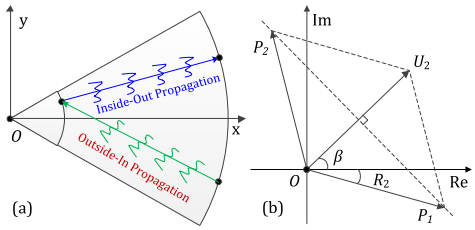

FIGURE 1. Principles of (a) cylindrical diffraction and (b) EMD.

respectively, and ICDT$\{\cdot\}$ denotes an inverse CDT. Here, CDT denotes a cylindrical diffraction transform, as shown in Fig. 1(a), and the point pulse function of CDT [47] can be expressed as

$$\begin{aligned} h(\theta, z, r_1, r_2) &= \frac{r_2 - r_1\cos\theta}{i\lambda L^2} \times \exp(i2\pi L/\lambda), \\ L &= [r_1^2 + r_2^2 - 2r_1 r_2\cos\theta + z^2]^{1/2}, \end{aligned} \quad (2)$$

where λ is the wavelength of the incident light, r_1 and r_2 denote the radii of the input and output cylindrical surfaces, respectively. Since the point pulse function h is given, it is easy to calculate U_2 or U_1 by using convolution algorithm as $U_1 = \mathrm{CDT}(U_2) = h \otimes U_2 = \mathrm{IFFT}[\mathrm{FFT}(h) \times \mathrm{FFT}(U_2)]$ and $\overline{U}_2 = \mathrm{ICDT}(U_1) = \mathrm{IFFT}[\mathrm{FFT}(U_1)/\mathrm{FFT}(h)]$, where $\otimes$ denotes convolution, FFT and IFFT are fast Fourier transform and inverse FFT, respectively [47].

In the conventional EMD, a complex amplitude can be treated as a vector in a two-dimensional Cartesian coordinate system. Here, the real (Re) and imaginary (Im) parts are horizontal and vertical components, respectively. For simplification, the coordinates will be omitted hereafter this paper. As shown in Fig. 1(b), U_2 is divided into two masks, P_1 and P_2, with equal modulus. This newly constructed distribution of complex amplitude can be rewritten as

$$\begin{aligned} U_2 &= A \times \exp(i\beta) = P_1 + P_2, \\ A &= \mathrm{abs}\{U_2\}, \quad \beta = \arg\{U_2\}, \end{aligned} \quad (3)$$

where A and β are the amplitude and phase angle of U_2, respectively. abs$\{\cdot\}$ and arg$\{\cdot\}$ denote the absolute and argument of a function, respectively. If an RPM distributed uniformly in the interval $[0, 2\pi]$ R_2 is expressed as

$$R_2 = 2\pi \times \mathrm{rand}() = \arg\{P_1\}, \quad (4)$$

where rand() denotes a random function, the masks P_1 and P_2 are deduced as

$$\begin{aligned} P_1 &= C \times \exp(iR_2), \quad C = 0.5A \times [\cos(\beta - R_2)]^{-1}, \\ P_2 &= C \times \exp(iPK), \quad PK = 2\beta - R_2 = \arg\{P_2\}. \end{aligned} \quad (5)$$

In this way, U_2 is hidden into two masks by emp$\otimes$loying an argument distribution R_2. With masks $[P_1, P_2]$, the original image can be reconstructed as

$$I = |\mathrm{CDT}\{U_2\}|^2 = |\mathrm{CDT}\{P_1 + P_2\}|^2. \quad (6)$$

However, the masks of P_1 and P_2 are complex-valued, it is not convenient for transmission or storage. Therefore,

we propose an IEMD which replaces the outputs of P_1 and P_2 by C andPK, respectively. Noted that, C andPK are both real-valued. Therefore, U_2 is hidden into two masks of [C,PK] successfully. With masks [C,PK], the original image can be retrieved from the following equation:

$$I = |\mathrm{CDT}\{U_2\}|^2 = \left|\mathrm{CDT}\left\{C\left[\exp(iR_2)+\exp(iPK)\right]\right\}\right|^2. \quad (7)$$

Obviously, it is easy to compute C from I by given R_1 and R_2. I can only be obtained from C when PK is used. However, if anyone attempts to achieve I without using PK, and even with R_1 and R_2, the result is bound to be a failure. Since a novel function of one-way trapdoor is created between I and C since PK acts as the trapdoor, an asymmetric cryptosystem is successfully accomplished with R_2 as the public key, PK as the private key, and C as the ciphertext. Note that, R_1 need not in decryption and could be any random function, while R_2 need for decryption and can also be generated by a chaos algorithm [48].

B. IMPLEMENTATIONS

The flowcharts of the encryption and decryption processes are shown in Figs. 2(a)-(b), respectively. For highly secure verification, ciphertext C and private key PK can be assigned to two users with different authorities, while the system parameters, such as the diffraction parameters and the two RPMs, remain constants in the verification system. Since the retrieved image can be achieved simply at the output plane only when C and PK are right at the same time, the decryption process can be implemented either optically or digitally. However, the encryption process should be partly implemented digitally since the obtaining of C and PK according to Eq. (5) is also hard to implemented optically.

The optical decryption system is schematically shown in Fig. 2(c). Firstly, two coherent light beams carrying information of ciphertext C which is split by a BS are modulated by two phase-only masks R_2 and PK. And then the modulated results of P_1 and P_2 are combined by an HM. After cylindrical diffraction of the combined result U_2, the diffraction result is the reconstructed image which can be captured by a CCD camera.

C. THEORETICAL ANALYSIS OF SECURIT

As a proposed asymmetric cryptosystem, it should be proved whether it meets all the five requirements of an asymmetric cryptosystem [18]. Let's study the five requirements one by one. Firstly, there are a pair of keys: public key (R_2) and the private key (PK), which are easy to obtain. Secondly, it is easy to obtain the ciphertext (C) when the public key (R_2) and plaintext (I) are already available. Thirdly, it is easy to reconstruct plaintext (I) by using the private key (PK). Fourthly, it is still difficult to conjecture the private key (PK) even if an opponent knew the public key (R_2). Fifthly, it is still difficult to reconstruct plaintext (I) even if an opponent knew the public key (R_2) and the ciphertext (C). Based on the above analysis, we can summarize that the proposed cryptosystem belongs to asymmetric cryptosystem.

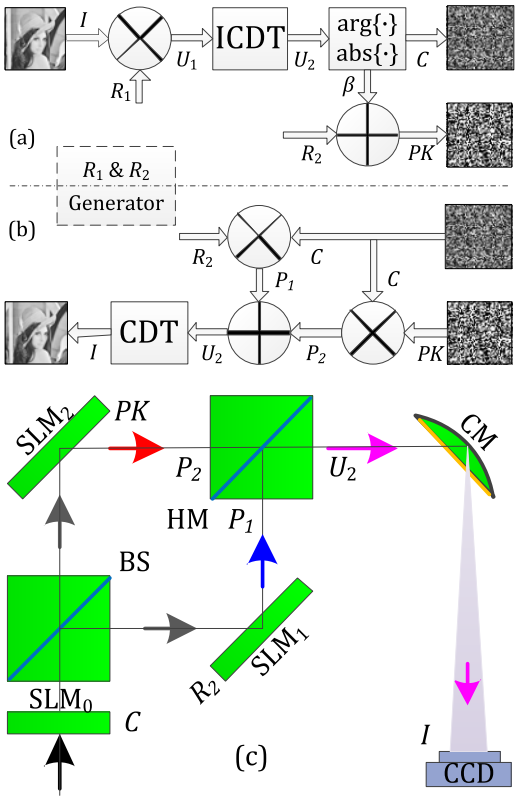

FIGURE 2. Asymmetric optical cryptosystem: Flowcharts of (a) encryption and (b) decryption processes. (c) Schematic of optical decryption process. Optical elements of SLM, BS, HM, CM, and CCD are spatial light modulator, beam splitter, half mirror, cylindrical mirror, and charge-coupled device, respectively.

Since the proposed cryptosystem introduces the cylindrical diffraction which is an asymmetric process of inside-out and outside-in propagation between two concentric cylinders [45], [46], it can resist the two IRA-based special attacks [35], [36] which the conventional EMD based cryptosystems are vulnerable to.

Moreover, the proposed cryptosystem has additional merit that it is easy for storage or transmission due to the real-valued outputs of the pure amplitude ciphertext and the pure phase private key.

III. SIMULATION RESULTS AND SECURITY ANALYSIS

The computer simulations are performed using Matlab R2010b platform with Processor Intel ®Core ^{TM}i7 @ 2.4 GHz, Memory 8.0 GB RAM, and 64-bit OS Win10 to verify our proposed scheme. The size of the test image is 512×512 pixels. The wavelength employed in cylindrical diffraction is $\lambda = 96$ um, which is in the far-infrared spectral region, the height of the cylinder is 64 mm, and the radii of r_1 and r_2 are 10 mm and 100 mm for the inner and outer cylinders, respectively [47].

In general cryptanalysis, it is assumed that everything of the cryptosystem is known to the attacker except the private key. Specifically, the attacker has known public key, the ciphertext, and even the encryption algorithm as well

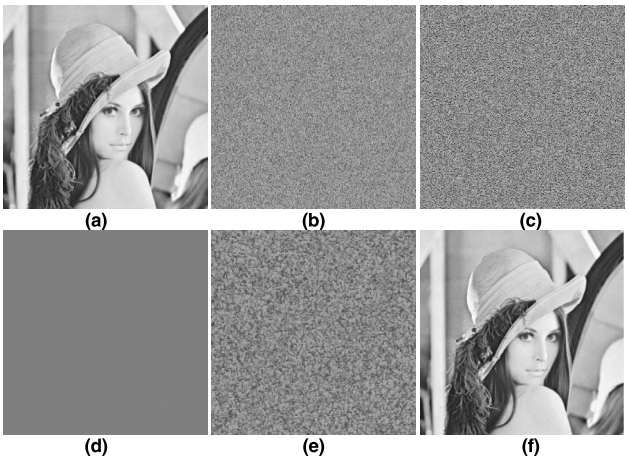

FIGURE 3. (a) Original image, (b) R_1, (c) R_2, (d) ciphertext C, (e) private key PK, and (f) decryption result with matched public and private keys.

as the diffraction parameters. It will be verified that the proposed cryptosystem can resist some attacks based on this assumption. The attacks to carry out are the brute force attack, the symmetric attacks, the silhouette problem, and the IRA-based specific attacks.

Besides the security performance, we also compare the encryption time, optical decryption complexity, and data amount of storage or transmission of our proposed method with the methods in literature 2015OL [34], 2016OLT [43] and 2017OLT [40].

To evaluate the reconstruction quality of the encryption and decryption method, the correlation coefficient CC between the reconstructed image (I_R) and the original image (I) is calculated as

$$CC = [\mathrm{cov}(I, I_R)]/(\sigma_I \times \sigma_{I_R}), \tag{8}$$

where cov denotes the cross-covariance, and σ denotes standard deviation.

A. ENCRYPTION AND DECRYPTION RESULTS

The encrypting image is a gray image Lena as shown in Fig. 3(a). Figs. 3(b)-(c) show R_1 and the public key R_2, respectively. Figs. 3(d)-(e) show the ciphertext C and private key PK, respectively. Fig. 3(f) shows the reconstructed image with the right public and private keys as well as the correct system parameters. The encryption results show that the plaintext image has successfully been hidden into two real-valued masks which are white noise and do not show any information about the original image. The simulation result shows that the original image has been retrieved completely because the corresponding value of CC is 1.00. Therefore, the original image can be reconstructed with high quality.

B. BRUTE FORCE ATTACK

The brute force attack of our cryptosystem can be demonstrated through key sensitivity and space by assuming that the values of phase keys are influenced with deviations. It can be

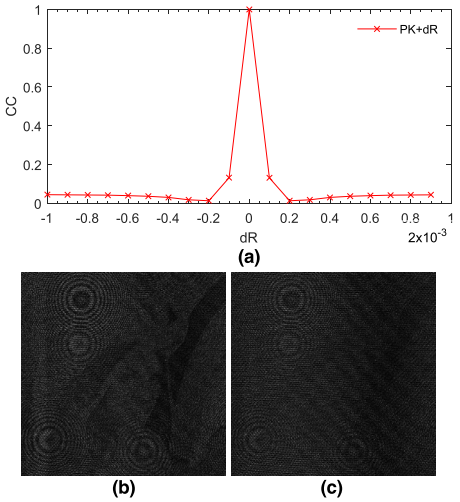

FIGURE 4. CC curve using different values of dR (a) compensating for PK. Decrypted results of (b) dR = 0.2 × PK × 10^{-3}, (c) dR = 0.4 × PK × 10^{-3}.

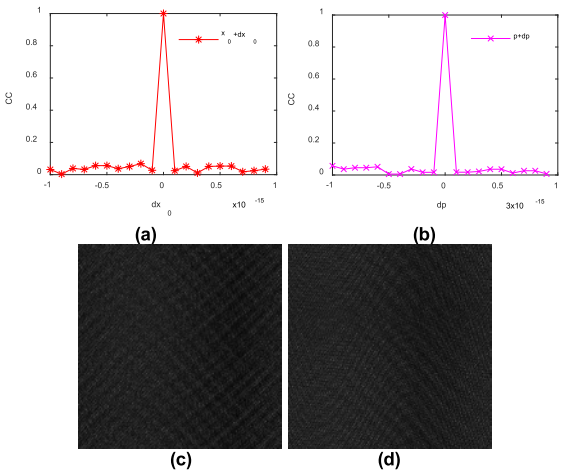

FIGURE 5. CC curve using different values compensating to (a) x_0, (b) p, decrypted results of (c) $dx_0 = 0.1 \times 10^{-15}$, (d) $dp = 0.3 \times 10^{-15}$.

represented by

$$P' = P + dR, \tag{9}$$

where P represents the correct phase key PK or public key R_2, dR denotes the deviation from their correct value, and P' is the phase value used for decryption. A series of CC values can be obtained according to various values of dR.

Figure 4(a) shows the CC curve using a different value of dR compensating for private key PK, the decrypted results of $dR = 0.2\times PK \times 10^{-3}$ and $dR = 0.4\times PK \times 10^{-3}$ are shown in Figs. 4(b)-(c), and the corresponding CC values are 0.132 and 0.014, respectively. The public key R_2 can be generated by a chaos algorithm [48] and is noted as $R_2(x_0, p)$, which is sensitive to x_0 and p. Figs 5(a) and (b) show the CC curve using a different value of dx_0 and dp compensating for parameters x_0 and p of public key R_2, respectively. the decrypted results of $dx_0 = 0.1 \times 10^{-15}$ and $dp = 0.3 \times 10^{-15}$ are shown in Figs. 5(c)-(d), respectively. Since the private key

FIGURE 6. Decrypted results of the ciphertext noisy by different strength of Gaussian noise. (a) 0.002, (b) 0.005, (c) 0.01.

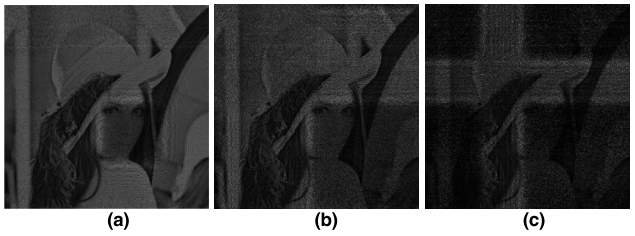

FIGURE 7. Decrypted results of the ciphertext images occluded at the top-left corner with (a) 6.25%, (b) 25.00%, (c) 56.25%.

PK is related to the public key R_2, it can be summarized that the key space is much greater than 8.3×10^{34}. Therefore, high robustness against a brute force attack is verified.

C. NOISE AND OCCLUSION ATTACKS

Figure 6 shows the decrypted results of the ciphertext noisy by different strength of Gaussian noise. The noisy model is given by

$$C' = C(1 + s \times G), \tag{10}$$

where G is Gaussian noise with zero-mean and 0.01 standard deviation, and s notes the noise strength. Figs. 6(a)-(c) are the results with strength of 0.002, 0.005, and 0.01, and the corresponding *CC* values are 0.847, 0.338, and 0.282, respectively.

Figures 7(a)-(c) show the decrypted results of Lena when ciphertexts are occluded at the top-left corner with 6.25%, 25.00%, and 56.25%, and the corresponding CC values are 0.7078, 0.4366, and 0.2954, respectively. Note that, the information of original image is just recognizable even up to 50% area loss. The occlusion effect on the ciphertext image is further studied by plotting CC values varying with occluded area as shown in Fig. 8, which verifies the robustness of the proposed cryptosystem.

D. SYMMETRIC ATTACK

Since different private keys will generate different ciphertexts, the proposed cryptosystem will resist the attacks that other symmetric DRPE cryptosystems are vulnerable to. Generally, these attacks are known-plaintext, chosen-plaintext, and chosen-ciphertext attacks [15]–[17]. To verify it, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks are carried out. Figs. 9(a)-(c) shows the decrypted image, which shows no useful information.

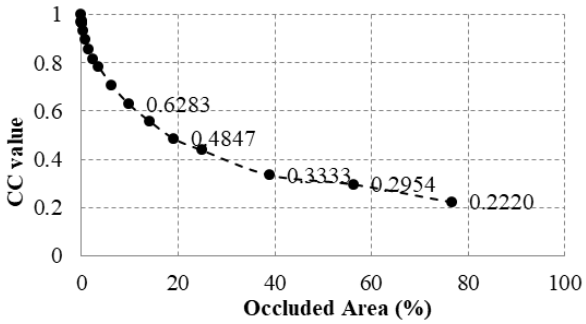

FIGURE 8. Plot of CC values against percentage occluded area.

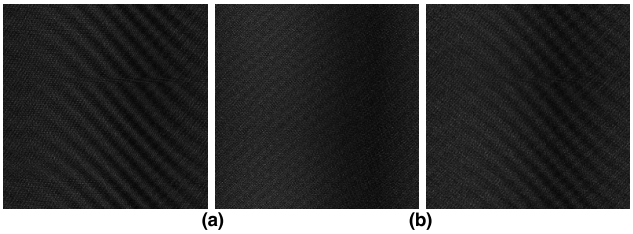

FIGURE 9. Decryption results of (a) know-plaintext attack, (b) chosen-plaintext attack, and (c) chosen-ciphertext attack.

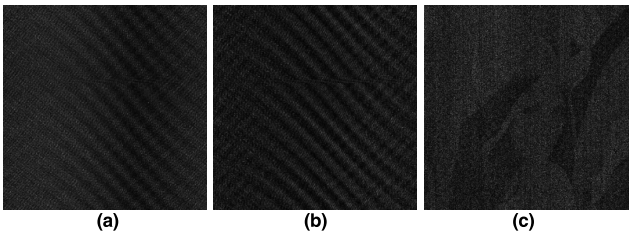

FIGURE 10. Decryption results of using only (a) C and (b) PK. Decryption result of only using one mask in [24].

E. SILHOUETTE PROBLEM

To verify the silhouette problem, attacks by using only C or PK is carried out. Figs. 10(a)-(b) show the direct decrypted results of using only C or PK, respectively. The decrypted results both are white noise, which doesn't show any information on the plaintext image. The corresponding *CCs* of Figs. 10(a)-(b) are 0.046 and 0.044, respectively. While the silhouette problem is shown as Fig. 10(c) when it is decrypted by using only one of the masks for the encryption method in [24]. Therefore, our proposed system does not have a silhouette problem.

F. SPECIFIC ATTACK

The verification of the IRA-based specific attack [35] and attack [36] is performed with our proposed method and method in 2015OL [34], respectively. Here, C and R_2 are given, and PK is randomly initialized to attack our proposed method. To verify it can withstand the specific attack, the CC value is used to show the convergence of iteration. As shown in Figs. 11(a)-(b), the relations between iteration times and the *CC*s (between I_k and I) are fluctuant and stay very low level, which illustrate the poor convergence of the attack [35]

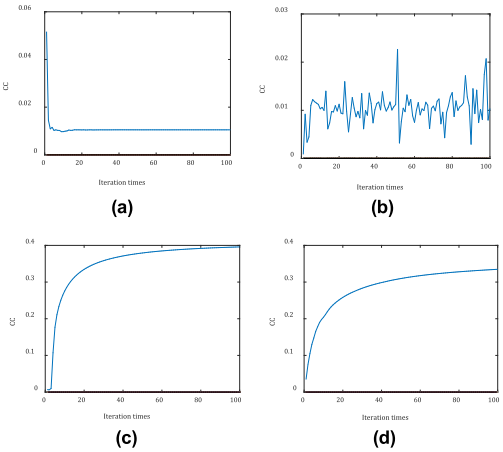

FIGURE 11. Relations between iteration times and CCs of IRA-based special (a) attack [35], (b) attack [36] to proposed; and (c) attack [35], (d) attack [36] to 2015OL [34].

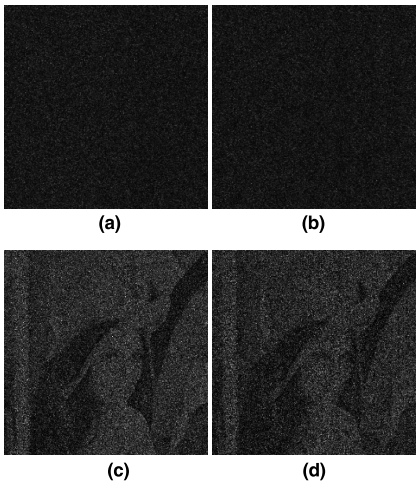

FIGURE 12. Results of IRA-based special (a) attack [35], (b) attack [36] to proposed, and (c) attack [35], (d) attack [36] to 2015OL [34].

and attack [36] to the proposed method. While Figs. 11(c)-(d) indicate that the method 2015OL [34] is vulnerable to these attacks.

To clarify the attack effect comparison further, the image results of attacks to the proposed method and the method 2015OL [34] are shown in Figs. 12(a)-(d) for attacks methods of attack [35] and attack [36]. Therefore, the proposed method can resist against the IRA-based specific attacks. Since the only difference is the proposed method replaces the Fourier transform by cylindrical diffraction transform compared with the method 2015OL [34], it shows that the asymmetric diffraction process of cylindrical diffraction ensures the proposed scheme free of IRA-based special attacks successfully.

G. Encryption TIME & DECRYPTION COMPLEXITY

The comparisons of encryption time and optical decryption complexity are shown in Tables 1 and 2, respectively.

The results of encryption time are average of carrying out 100 times. The encryption time of our proposed method is slightly longer than that of the method in 2015OL [34] and much shorter than these of methods in 2016OLT [43] and 2017OLT [40].

TABLE 1. Comparison of encryption times.

	Image resolution 512×512			
	Proposed	2015OL [34]	2016OLT [43]	2017OLT [40]
Encryption time (ms)	96.3	88.3	128.5	125.6

TABLE 2. Comparison of decryption complexity.

Decryption complexity	Image resolution 512×512			
	Proposed	2015OL [34]	2016OLT [43]	2017OLT [40]
Numbers of SLMs	3	4	6	6

TABLE 3. Comparison of amount of storage or transmission.

Data Amount	Data amount (Unit: Image resolution)			
	Proposed	2015OL [34]	2016OLT [43]	2017OLT [40]
Ciphertext	1	2	2	1
Keys	1	2	4	5

To simplify the indication of optical decryption complexity, the number of SLMs used in these methods is employed. Supposing a modulation of a complex amplitude needs two SLMs. And the results are shown in Table 2. It shows that the optical decryption complexity of our proposed method is slightly smaller than that of the method of 2015OL [34] and is much smaller than those of the other two methods of 2016OLT [43] and 2017OLT [40].

H. DATA AMOUNT OF STORAGE OR TRANSMISSION

The data amount of storage or transmission is another important aspect of the cryptosystem. The comparison of the data amount of storage or transmission of these cryptosystems is shown in Table 3. To simplify the comparison, the image resolution is employed as the unit of data amount. Since the public key R_2 can be generated by chaos algorithm, the data amount of the keys of our proposed method is 1, which is just the phase key. And the data amount of the ciphertext of our proposed method is also 1 due to real-valued output. From the results of data amount shown in Table 3, the total data amount of our proposed method is much smaller than those of the methods in literature 2015OL [34], 2016OLT [43] and 2017OLT [40].

From the above analysis, the proposed system is free of the silhouette problem and ensures high-level security to the special attack based on IRAs, brute force attack, as well as symmetric attacks, such as known-plaintext, chosen-plaintext, and chosen-ciphertext attacks.

In addition, our proposed method has comparative advantages on encryption time, optical decryption complexity, and the data amount of storage or transmission compared with the other methods in [34], [43], and [40]. Furthermore, our proposed method has merits compared with the typical DRPE based encryption [5] and the DRPE based encryption in cylindrical diffraction domain [45]. This proposed cryptosystem employees only single cylindrical diffraction and is a cryptosystem with asymmetric keys. These two features ensure merits of simpler optical implementation and higher security compared with [5] and [45], respectively.

IV. CONCLUSIONS

In this paper, an asymmetric cryptosystem based on IEMD in cylindrical diffraction domain has been presented, which provides a novel function of one-way trapdoor for an asymmetric cryptosystem. The proposed cryptosystem is free of silhouette problem and special attack based on IRAs, which is mainly due to the introduction of cylindrical diffraction. Furthermore, it is convenient for storage or transmission due to the real-valued outputs of the proposed IEMD. In addition, our proposed method has comparative advantages on encryption time, optical decryption complexity, and the data amount of storage or transmission compared with the other methods in the literature [34], [43], and [40]. The validity of the proposed cryptosystem has been verified by the computer simulations.

REFERENCES

[1] Y. Geng *et al.*, "Computational coherent imaging by rotating a cylindrical lens," *Opt. Express*, vol. 26, no. 17, pp. 22110–22122, Aug. 2018.
[2] 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.
[3] 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, Jun. 2000.
[4] 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.
[5] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, Jul. 2004.
[6] L. Chen and D. Zhao, "Optical image encryption with Hartley transforms," *Opt. Lett.*, vol. 31, no. 23, pp. 3438–3440, Dec. 2006.
[7] X. C. Cheng *et al.*, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett.*, vol. 33, no. 14, pp. 1575–1577, Jul. 2008.
[8] M. Cho and B. Javidi, "Three-dimensional photon counting double-random-phase encryption," *Opt. Lett.*, vol. 38, no. 17, pp. 3198–3201, Sep. 2013.
[9] K. Falaggis, A. H. R. Andrade, J. G. G. Luna, C. G. Ojeda, and R. Porras-Aguilar, "Optical encryption with protection against dirac delta and plain signal attacks," *Opt. Lett.*, vol. 41, no. 20, pp. 4787–4790, Oct. 2016.
[10] A. V. Zea, J. F. B. Ramirez, and R. Torroba, "Optimized random phase encryption," *Opt. Lett.*, vol. 43, no. 15, pp. 3558–3561, Aug. 2018.
[11] Z. Liu, J. Tan, W. Liu, J. Wu, Q. Wu, and S. Liu, "A diffraction model of direction multiplexing method for hiding multiple images," *J. Mod. Opt.*, vol. 61, no. 14, pp. 1127–1132, 2014.
[12] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Fully phase image encryption using double random-structured phase masks in gyrator domain," *Appl. Opt.*, vol. 53, no. 28, pp. 6472–6481, Oct. 2014.
[13] H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane," *Opt. Lasers Eng.*, vol. 67, pp. 145–156, Apr. 2015.
[14] H. Singh, "Nonlinear optical double image encryption using random-optical vortex in fractional Hartley transform domain," *Opt. Appl.*, vol. 47, no. 4, pp. 557–578, 2017.
[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] Y. S. Zhang, D. Xiao, W. Y. Wen, and H. Liu, "Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding," *Opt. Lett.*, vol. 38, no. 21, pp. 4506–4509, Nov. 2013.
[17] 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.
[18] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, 2010.
[19] X. Wang and D. Zhao, "Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask," *Opt. Lett.*, vol. 38, no. 18, pp. 3684–3686, Sep. 2013.
[20] X. Wang and D. Zhao, "Simultaneous nonlinear encryption of grayscale and color images based on phase-truncated fractional Fourier transform and optical superposition principle," *Appl. Opt.*, vol. 52, no. 25, pp. 6170–6178, Sep. 2013.
[21] B. Cao, J. Li, and Z. Huang, "Phase-only asymmetric encryption based on coherent superposition and phase-truncated Fourier transforms," *Opt. Commun.*, vol. 347, pp. 118–122, Jul. 2015.
[22] X. Wang, Y. Chen, C. Dai, and D. Zhao, "Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform," *Appl. Opt.*, vol. 53, no. 2, pp. 208–213, Jan. 2014.
[23] Y. Xiong, A. He, and C. Quan, "Cryptanalysis of an optical cryptosystem based on phase-truncated Fourier transform and nonlinear operations," *Opt. Commun.*, vol. 428, pp. 120–130, Dec. 2018.
[24] Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.*, vol. 33, no. 21, pp. 2443–2445, Nov. 2008.
[25] W. Chen, C. Quan, and C. J. Tay, "Optical color image encryption based on arnold transform and interference method," *Opt. Commun.*, vol. 282, no. 18, pp. 3680–3685, Sep. 2009.
[26] C. H. Niu, X. L. Wang, N. G. Lv, Z. H. Zhou, and X. Y. Li, "An encryption method with multiple encrypted keys based on interference principle," *Opt. Express*, vol. 18, no. 8, pp. 7827–7834, Apr. 2010.
[27] W. Jia, F. J. Wen, Y. T. Chow, and C. Zhou, "Binary image encryption based on interference of two phase-only masks," *Appl. Opt.*, vol. 51, no. 21, pp. 5253–5258, Jul. 2012.
[28] S. K. Rajput and N. K. Nishchal, "Image encryption based on interference that uses fractional Fourier domain asymmetric keys," *Appl. Opt.*, vol. 51, no. 10, pp. 1446–1452, Apr. 2012.
[29] Q. Wang, Q. Guo, L. Lei, and J. Zhou, "Single-beam image encryption using spatially separated ciphertexts based on interference principle in the Fresnel domain," *Opt. Commun.*, vol. 333, pp. 151–158, Dec. 2014.
[30] X. Wang and D. Zhao, "Optical image hiding with silhouette removal based on the optical interference principle," *Appl. Opt.*, vol. 51, no. 6, pp. 686–691, 2012.
[31] W. Chen and X. Chen, "Iterative phase retrieval for simultaneously generating two phase-only masks with silhouette removal in interference-based optical encryption," *Opt. Commun.*, vol. 331, pp. 133–138, Nov. 2014.
[32] Y. Qin, H. Wang, Z. Wang, Q. Gong, and D. Wang, "Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal," *Opt. Lasers Eng.*, vol. 84, pp. 62–73, Sep. 2016.
[33] S. Liansheng, Z. Xiao, H. Chongtian, T. Ailing, and A. K. Asundi, "Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms," *Opt. Lasers Eng.*, vol. 113, pp. 29–37, Feb. 2019.
[34] J. Cai, X. Shen, M. Lei, C. Lin, and S. Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Lett.*, vol. 40, no. 4, pp. 475–478, Feb. 2015.
[35] X. Deng, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition: Comment," *Opt. Lett.*, vol. 40, no. 16, p. 3913, Aug. 2015.
[36] J. Wu, W. Liu, Z. Liu, and S. Liu, "Cryptanalysis of an 'asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition,'" *Appl. Opt.*, vol. 54, no. 30, pp. 8921–8924, Oct. 2015.

[37] J. Cai, X. Shen, and C. Lin, "Security-enhanced asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Commun.*, vol. 359, pp. 26–30, Jan. 2016.
[38] S. P. Barfungpa and M. R. Abuturab, "Asymmetric cryptosystem using coherent superposition and equal modulus decomposition of fractional Fourier spectrum," *Opt. Quantum Electron.*, vol. 48, no. 11, p. 520, Nov. 2016.
[39] R. Girija and H. Singh, "Symmetric cryptosystem based on chaos structured phase masks and equal modulus decomposition using fractional Fourier transform," *3D Res.*, vol. 9, no. 3, p. 42, 2018.
[40] J. Cai and X. Shen, "Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition," *Opt. Laser Technol.*, vol. 95, pp. 105–112, Oct. 2017.
[41] H. Chen, C. Tanougast, Z. Liu, and L. Sieler, "Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains," *Opt. Lasers Eng.*, vol. 93, pp. 1–8, Jun. 2017.
[42] H. Xu, W. Xu, S. Wang, and S. Wu, "Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain," *Opt. Commun.*, vol. 402, pp. 302–310, Nov. 2017.
[43] L. Chen, X. Gao, X. Chen, B. He, J. Liu, and D. Li, "A new optical image cryptosystem based on two-beam coherent superposition and unequal modulus decomposition," *Opt. Laser Technol.*, vol. 78, pp. 167–174, Apr. 2016.
[44] R. Kumar, B. Bhaduri, and N. K. Nishchal, "Nonlinear QR code based optical image encryption using spiral phase transform, equal modulus decomposition and singular value decomposition," *J. Opt.*, vol. 20, no. 1, Dec. 2017, Art. no. 015701.
[45] J. Wang, X. Li, Y. Hu, and Q. H. Wang, "Phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and double-random phase encoding," *Opt. Commun.*, vol. 410, pp. 468–474, Mar. 2018.
[46] J. Wang, Q. H. Wang, and Y. Hu, "Image encryption using compressive sensing and detour cylindrical diffraction," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–14, Jun. 2018.
[47] J. Wang, Q. H. Wang, and Y. Hu, "Unified and accurate diffraction calculation between two concentric cylindrical surfaces," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 35, no. 1, pp. A45–A52, Jan. 2018.
[48] X. Wang, J. Zhao, and H. Liu, "A new image encryption algorithm based on chaos," *Opt. Commun.*, vol. 285, no. 5, pp. 562–566, Mar. 2012.

JUN WANG received the Ph.D. degree from the Department of Electronic and Computer Engineering, Hanyang University, Seoul, South Korea, in 2011. He was a Postdoctoral Fellow with the University of Wisconsin-Madison, Madison, WI, USA, from 2011 to 2012. He has been a short-time Visiting Scholar with the School of Instrumentation and Optoelectronic Engineering, Beihang University, since 2018. He has been an Associate Professor with the College of Electronics & Information Engineering, Sichuan University, Chengdu, China, since 2012. He has published more than 40 publications. His current research interests include image encryption, holographic 3D display, and image processing.

XUDONG CHEN is currently pursuing the M.S. degree with the College of Electronics & Information Engineering, Sichuan University, Chengdu, China. His research interests include image encryption and data security.

JIANQING ZENG is currently pursuing the M.S. degree with the College of Electronics & Information Engineering, Sichuan University, Chengdu, China. Her research interests include image encryption and data security.

QIONG-HUA WANG received the M.S. and Ph.D. degrees from the University of Electronic Science and Technology of China (UESTC), in 1995 and 2001, respectively. She was with the UESTC, from 1995 to 2001. She was a Postdoctoral Research Fellow with the School of Optics/CREOL, University of Central Florida, from 2001 to 2004. She was a Professor with the School of Electronics and Information Engineering, Sichuan University, from 2004 to 2018. She is currently a Professor of optics with the School of Instrumentation and Optoelectronic Engineering, Beihang University. She published approximately 200 papers cited by Science Citation Index and authored two books. She holds five U.S. patents and 100 Chinese patents. Her research interest includes optics and optoelectronics, especially display technologies. She is a fellow of the Society for Information Display and an Associate Editor of *Optics Express* and the *Journal of the Society for Information Display*.

YUHEN HU received the B.S.E.E. degree from National Taiwan University, Taipei, Taiwan, in 1976, and the M.S. and Ph.D. degrees in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1980 and 1982, respectively.

He was with the Electrical Engineering Department, Southern Methodist University, Dallas, TX, USA. He is currently a Professor with the Electrical and Computer Engineering Department, University of Wisconsin-Madison, Madison, WI, USA. He has authored more than 300 journal and conference papers and edited and coauthored several books. His current research interests include multimedia signal processing and communication, design methodology and implementation of embedded algorithms and systems, and nano-scale IC design methodologies.

Dr. Hu served as the Chair of the IEEE Multimedia Signal Processing Technical Committee and the IEEE Neural Network Signal Processing Technical Committee. He served as the Secretary of the IEEE Signal Processing Society and the Board of Governors of the IEEE Neural Networks Council. He served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING, the IEEE SIGNAL PROCESSING LETTERS, the JOURNAL OF VERY LARGE SCALE INTEGRATION SYSTEMS SIGNAL PROCESSING, the IEEE *Multimedia Magazine*, and the *European Journal of Applied Signal Processing*.