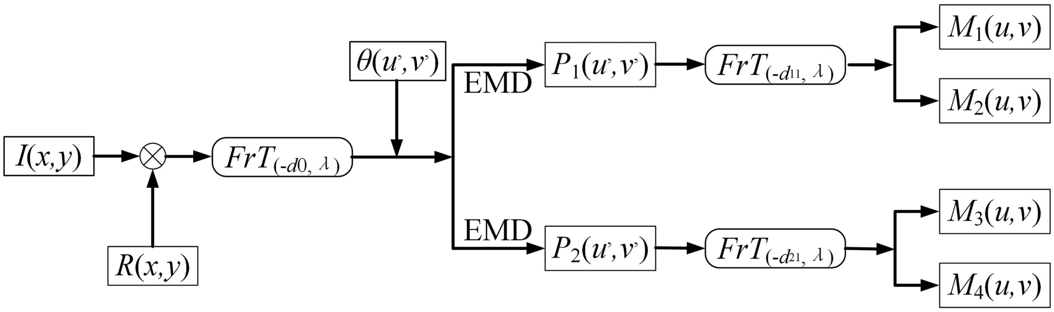
IEEE Photonics Journal
An IEEE Photonics Society Publication

Asymmetric Optical Image Encryption With Silhouette Removal Using Interference and Equal Modulus Decomposition

Volume 12, Number 2, April 2020

Guangyu Luan
Aichuan Li
Zhengguang Chen
Caojun Huang



DOI: 10.1109/JPHOT.2020.2963921

Asymmetric Optical Image Encryption With Silhouette Removal Using Interference and Equal Modulus Decomposition

Guangyu Luan, Aichuan Li, Zhengguang Chen, and Caojun Huang

College of Electrical and Information, Heilongjiang Bayi Agricultural University, Daqing,
Heilongjiang, 163319, China

DOI:10.1109/JPHOT.2020.2963921

Manuscript received November 22, 2019; accepted December 31, 2019. Date of publication January 2, 2020; date of current version March 9, 2020. This work was supported in part by the Education Department Foundation of Heilongjiang Province of China under Grant 12541584 and in part by the Natural Science Foundation of Heilongjiang Province of China under Grant C2018050. Corresponding author: Guangyu Luan (e-mail: luanguangyu@126.com).

Abstract: We propose an asymmetric optical image encryption scheme with silhouette removal by using interference and equal modulus decomposition (EMD). Plaintext is first separated into two complex value masks with the same modulus using EMD in the Fresnel transform domain. The two masks are encoded into four phase-only masks (POMs), two of which are treated as ciphertexts and other two as plaintext-dependent private keys by using the inverse Fresnel transform with different diffraction distances and interference-based encryption. Any information about the plaintext, including its silhouette, cannot be retrieved using one, two, or even three of the four POMs. Our scheme also avoids the constraint of the same modulus in EMD and eliminates the vulnerability against the iterative amplitude-phase attack and advanced iterative amplitude-phase attack. Numerical simulations were used to verify the validity and security of our proposed method.

Index Terms: Optical image encryption, asymmetric, silhouette problem, same modulus constraint.

1. Introduction

Optical image encryption [1]–[16] has made significant advances in recent decades. The interference-based encryption (IBE) scheme [17] proposed by Zhang and Wang is useful for optical image encryption because of its simple structure and an encryption process that does not involve iteration. In Zhang and Wang's method, an image is analytically encoded into two phase-only masks (POMs). In the decryption process, the silhouette of the original image can be revealed by one of two POMs. This inherent security defect has spawned a variety of silhouette removal methods [2], [18]–[21] for enhancing the security of encryption. One solution is to scramble the pixels of two POMs [18], [19] to solve the silhouette problem. However, the equipollent nature and symmetry of POMs persist. One proposal [20] is to encode the original image into three POMs. One of three POMs does not render the silhouette of the image but the other two do. Another proposal by Zhong *et al.* [2] can be used to eliminate the silhouette problem. However, the three POMs have the same decryption keys in this case, which hinders the enhancement in security. Moreover, Cai *et al.* [22] proposed an optical cryptosystem based on equal modulus decomposition (EMD) and coherent superposition to avoid the silhouette problem. However, the silhouette appears only if two parts of the phase of the masks are used, and this method is vulnerable to the iterative amplitude-phase attack (IAPA) [23] and advanced iterative amplitude-phase attack (AIAPA) [24]. Cai *et al.* [25] introduced full phase encryption to EMD to remove the silhouette problem and vulnerability against the IAPA, but the cryptosystem needs methods of extra phase contrast to record the decrypted image, which renders the cryptosystem challenging to implement via optical approaches. Apart from analytical solutions [17]–[22], [25], researchers have used the phase retrieval algorithm (PRA) [26]–[28] to overcome the problems of linearity and the silhouette. The PRA is an effective way to radically eliminate the equipollent nature of the POMs but is time consuming.

In this study, we propose an asymmetric method of optical image encryption that combines interference with EMD to generate four POMs. Two of the POMs are treated as ciphertexts and the other two as plaintext-dependent private keys, which makes the cryptosystem asymmetric. The four POMs and two diffraction distances in our proposed approach enlarge the key space. Moreover, the proposed approach can remove the silhouette problem analytically and relax the constraint of the same modulus in EMD. The results of simulations were used to verify the reliability of our method for image encryption.

2. Theoretical Analysis

In our encryption system, the plaintext $I(x, y)$ is first transferred to a complex value image and a Fresnel transform is performed on it:

$$S(u', v') = FrT_{(-d_0,\lambda)}\left\{\sqrt{I(x,y)}\exp\left[i2\pi R(x,y)\right]\right\} \tag{1}$$

where $FrT\{\}$ indicates the operation of the Fresnel transform, subscript d_0 represents the propagation distance between masks and the CCD plane, subscript λ represents the wavelength of the laser beams used for illumination, and $R(x, y)$ indicates a random function distributed uniformly over the interval [0, 1], and is used as a public key in our cryptosystem. (x, y) and (u', v') are coordinates of the image plane and the first Fresnel transform plane, respectively. The amplitude of $S(u', v')$ is $\mathrm{A}(u', v') = |\mathrm{S}(u', v')|$ and its phase as $Ph(u', v') = \varphi(u', v') = \arg[S(u', v')]$, where the operators $||$ and arg[] denote the modulus and the argument of the function, respectively.

As shown in Fig. 1, $S(u', v')$ is divided into two masks $P_1(u', v')$ and $P_2(u', v')$ with the same modulus. $\theta(u', v')$ can be represented by

$$\arg(P_1(u', v')) = \theta(u', v') = 2\pi\, rand(u', v') \tag{2}$$

where $\mathrm{rand}(u', v')$ represents a uniformly distributed random function on the interval [0, 1]. $\theta(u', v')$ acts as an encryption key. By geometrical deduction, $P_1(u', v')$ and $P_2(u', v')$ can be calculated by

$$P_1(u', v') = \frac{A(u', v')/2}{\cos\left[Ph(u', v') - \theta(u', v')\right]}\exp\left[i\theta(u', v')\right] \tag{3}$$

$$P_2(u', v') = \frac{A(u', v')/2}{\cos\left[Ph(u', v') - \theta(u', v')\right]}\exp\left\{i\left[2Ph(u', v') - \theta(u', v')\right]\right\} \tag{4}$$

Once $P_1(u', v')$ and $P_2(u', v')$ have been obtained, the inverse Fresnel transform is used with different diffraction distances, d_{11} and d_{21}, as:

$$S_1(u, v) = FrT_{(-d_{11},\lambda)}\left\{P_1(u', v')\right\} \tag{5}$$

$$S_2(u, v) = FrT_{(-d_{21},\lambda)}\left\{P_2(u', v')\right\} \tag{6}$$

where (u, v) denotes coordinates of the second Fresnel transform plane. $S_1(u, v)$ and $S_2(u, v)$ are then encoded into two POMs respectively using interference:

$$M_1(u, v) = \arg(S_1(u, v)) - \arccos(\left|S_1(u, v)\right|/2) \tag{7}$$

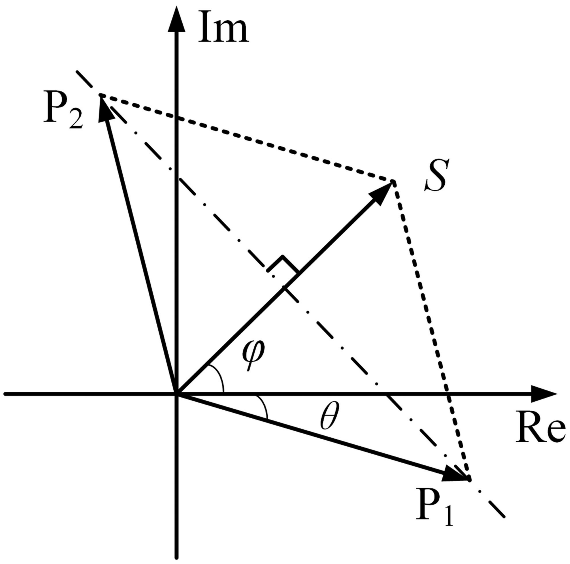


Fig. 1. EMD in the Fresnel transform domain.

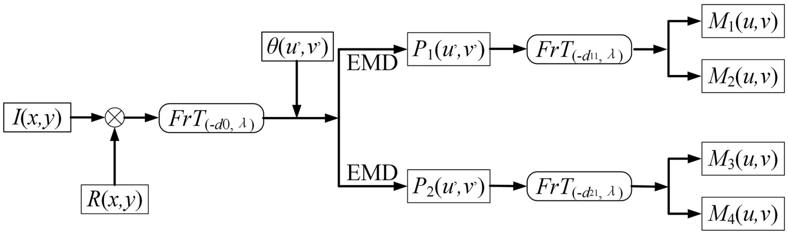


Fig. 2. Encryption procedure of our scheme.

$$M_2(u, v) = \arg(S_1(u, v) - \exp(iM_1(u, v))) \tag{8}$$

$$M_3(u, v) = \arg(S_2(u, v)) - \arccos(\left|S_2(u, v)\right|/2) \tag{9}$$

$$M_4(u, v) = \arg(S_2(u, v) - \exp(iM_3(u, v))) \tag{10}$$

The encryption procedure of our scheme is shown in Fig. 2 and our proposed optical decryption process is shown in Fig. 3. The light source with the corresponding wavelength λ illuminates M_1, M_2, M_3, and M_4 placed at prefixed places. An intensity detector is used to obtain the decrypted image, which is as follows:

$$I(x, y) = \left|FrT_{(d_1,\lambda)}[M_1(u, v)] + FrT_{(d_1,\lambda)}[M_2(u, v)] + FrT_{(d_2,\lambda)}[M_3(u, v)] + FrT_{(d_2,\lambda)}[M_4(u, v)]\right|^2 \tag{11}$$

where $d_1 = d_0 + d_{11}$ is the diffraction distance for M_1 and M_2, and $d_2 = d_0 + d_{21}$ is the diffraction distance for M_3 and M_4.

3. Numerical Simulation and Analysis

Numerical simulations were performed to verify the validity and security of our proposed method. The chosen axial distance d_0 was 50 mm, d_{11} was 50 mm, d_{21} was 40 mm, and the wavelength of a collimated plane wave was 633 nm. The original image "Lena" with 256 $\times$ 256 pixels and 256 gray levels was used as plaintext, and is shown in Fig. 4(a). The phase distributions of $R(x, y)$ and $\theta(u', v')$ are shown in Figs. 4(b) and 4(c), respectively. Using the proposed approach, the distribution of

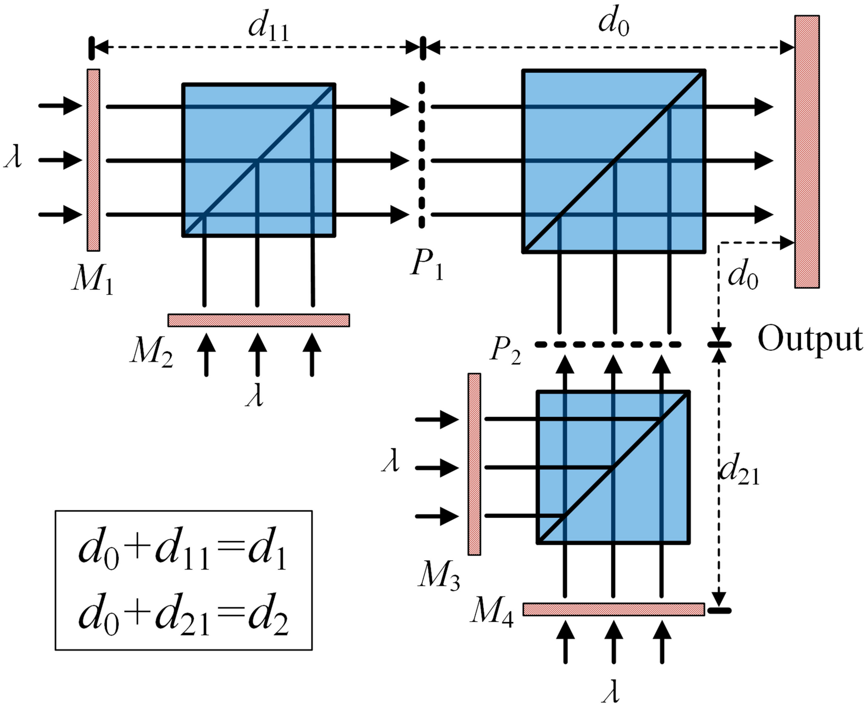


Fig. 3. Schematic of our optical decryption process.

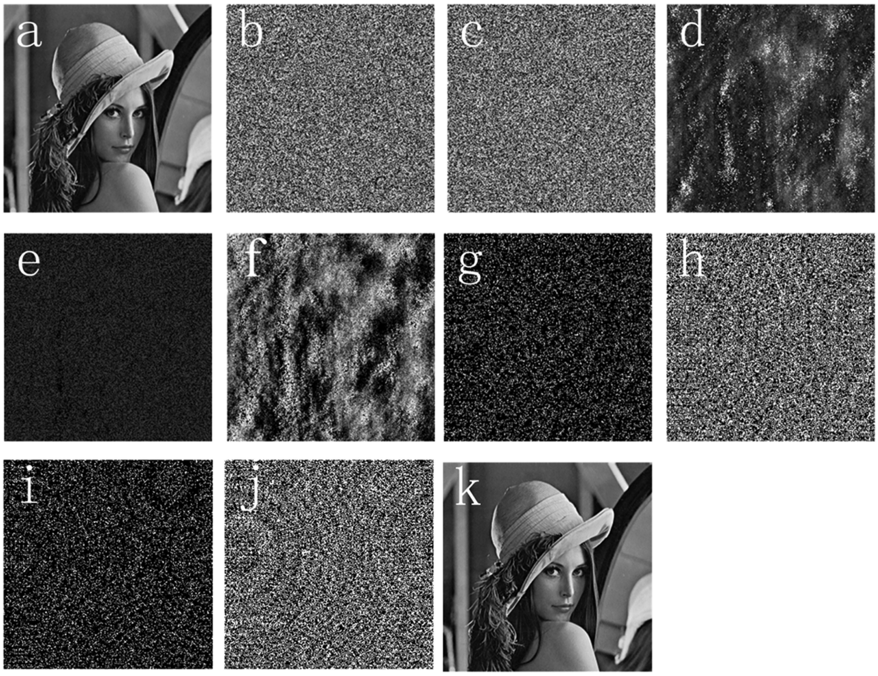


Fig. 4. The results of encryption and decryption for the proposed approach. (a) Plaintext. (b) Phase distribution of $R(x, y)$. (c) Phase distribution of $\theta(u', v')$. (d) Amplitude distribution of P_1 or P_2. (e) and (f) Phase distributions of P_1 and P_2 respectively. (g)–(j) M_1, M_2, M_3, and M_4 respectively. (k) Decrypted image.

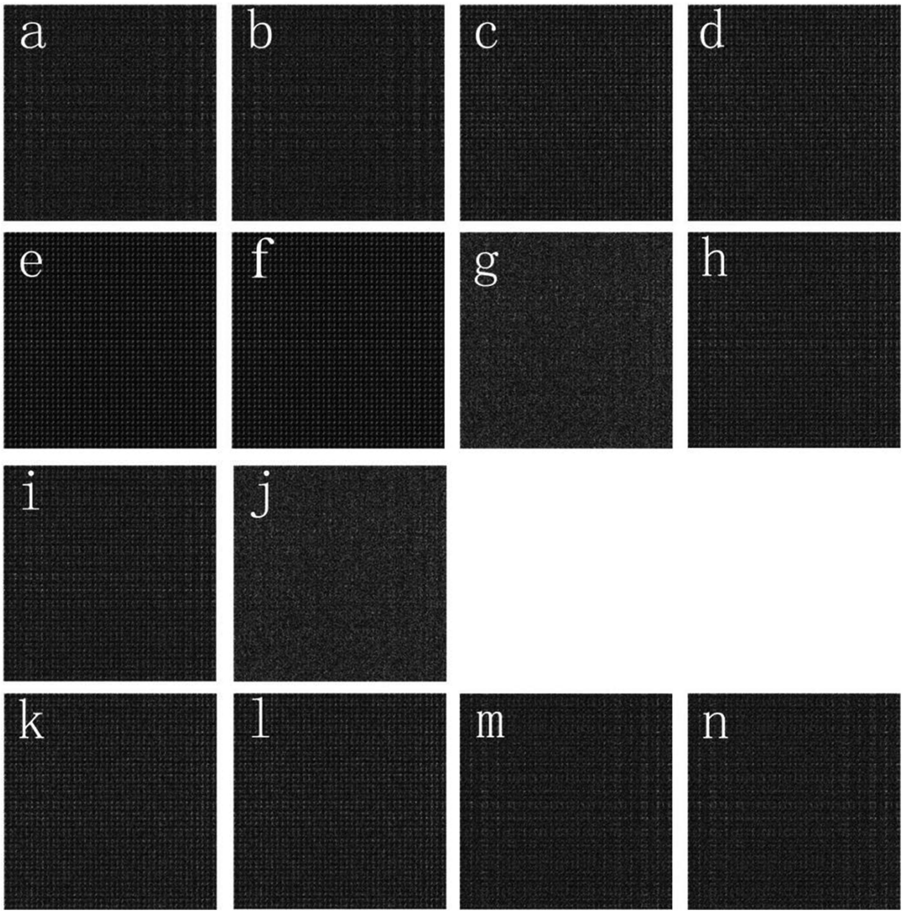


Fig. 5. The results of decryption with different conditions. (a)–(d) Decrypted images using one of M_1, M_2, M_3, and M_4, respectively. (e) Decrypted image using M_1 and M_2. (f) Decrypted image using M_3 and M_4. (g) Decrypted image using M_1 and M_3. (h) Decrypted images using M_1 and M_4. (i) Decrypted image using M_2 and M_3. (j) Decrypted image using M_2 and M_4. (k) Decrypted image using M_1, M_2, and M_3. (l) Decrypted image using M_1, M_2, and M_4. (m) Decrypted image using M_1, M_3, and M_4. (n) Decrypted image using M_2, M_3, and M_4.

the amplitude of P_1 or P_2 is shown in Fig. 4(d). The two-phase distributions of P_1 and P_2 are shown in Figs. 4(e) and 4(f), respectively. M_1, M_2, M_3 and M_4 were calculated as shown in Figs. 4(g)–4(j). The decrypted image was obtained by using all the appropriate keys and ciphertexts for decryption, as shown in Fig. 4(k).

To prove that the proposed approach can solve the silhouette problem in IBE, we used one of M_1, M_2, M_3 and M_4 for decryption, and the decrypted images are shown in Figs. 5(a)–5(d). Moreover, we used two of M_1, M_2, M_3 and M_4 for decryption, and the decrypted images are shown in Figs. 5(e)–5(j). Three of M_1, M_2, M_3 and M_4 were then used for decryption, the results are shown in Figs. 5(k)–5(n). In these results, any information concerning the plaintext, including its silhouette, is not observable.

To verify the sensitivity of the proposed approach to diffraction distances and the illuminating wavelength, the correlation coefficient (CC) [29] was used to calculate the difference between the original and the decrypted images:

$$CC = \frac{E\left\{[I_i - E[I_i]]\right\}\left\{[I_o - E[I_o]]\right\}}{E\sqrt{\left\{[I_i - E[I_i]]^2\right\}}\sqrt{\left\{[I_o - E[I_o]]^2\right\}}} \tag{12}$$

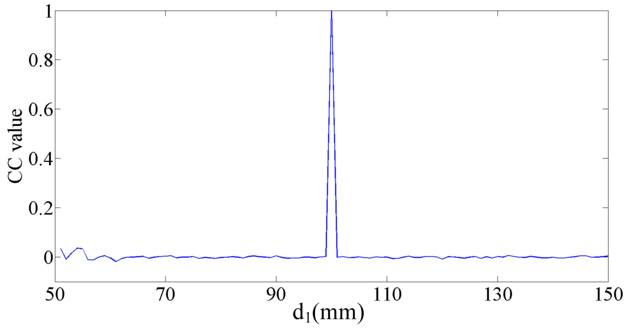


Fig. 6. Relation between the value of CC and d_1.

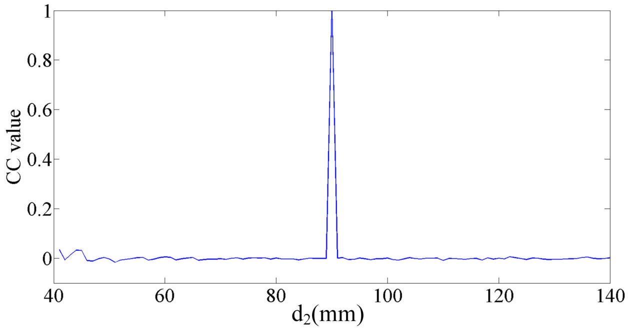


Fig. 7. Relation between the value of CC and d_2.

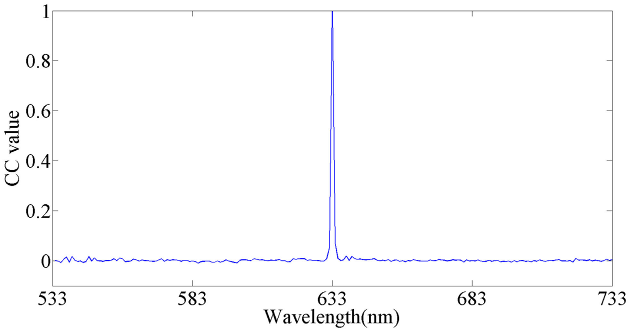


Fig. 8. Relation between the value of CC and the illuminating wavelength.

where I_i and I_o are the original image and the decrypted image, respectively. The relationships between the value of CC and the diffraction distance (d_1 or d_2) are shown in Figs. 6 and 7. The relation between CC and the illuminating wavelength is shown in Fig. 8. These results show that the sensitivities of the proposed approach to diffraction distances and the illuminating wavelength were so high that a slight deviation could lead to a failure to recognize the original image. In other words, the decrypted image could be obtained only when the correct diffraction distances and correct illuminating wavelength were used for decryption.

To further verify the robustness of the proposed approach against IAPA and AIAPA, we assumed that the ciphertexts (M_1 and M_2), public key $R(x, y)$, and decryption keys (d_1 and d_2) were all known for unauthorized intruders while the private keys (M_3 and M_4) and encryption keys (d_0, d_{11}, d_{21} and $\theta(u', v')$) were unknown for them. Figs. 9(a) and 9(b) give the decrypted images using

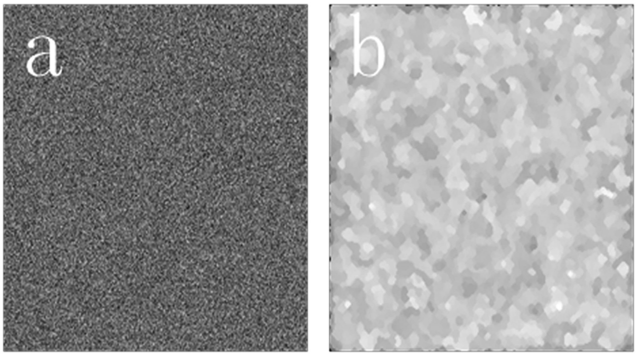


Fig. 9. Decrypted images. (a) IAPA. (b) AIAPA.

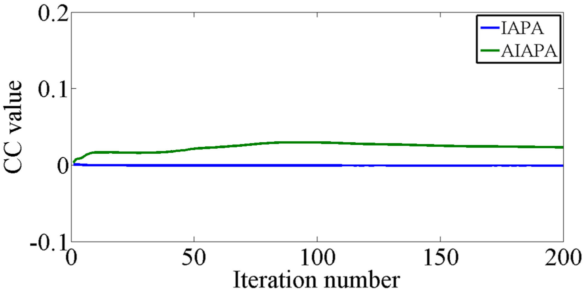


Fig. 10. The value of CC versus number of iterations in two attacks.

the IAPA and the AIAPA, respectively, and Fig. 10 gives the relations between the value of the CC and the number of iterations for IAPA and AIAPA. Decrypted images in the two attacks cannot be recognized, and the values of the CC were approximately zero in the two attacks even when the number of iteration was 200. These results prove that the proposed approach is robust against the IAPA and AIAPA.

4. Conclusion

In this paper, we proposed and tested an asymmetric method for optical encryption by using a combination of interference and EMD. EMD in the Fresnel transform domain was used to separate the plaintext into two complex value masks with the same modulus. Using the inverse Fresnel transform with different diffraction distances and interference-based encryption, the two masks were then divided into four POMs. The silhouette problem was solved using the four POMs. The proposed method enhances security by the four POMs and two diffraction distances. The results of numerical simulations show that our approach is sensitive to keys, and is robust against the IAPA and AIAPA. It provides a new solution to the problem of interference-based image encryption.

References

[1] A. Alfalou and C. Brosseau, “Recent advances in optical image processing,” *Prog Opt.*, vol. 60, pp. 119–262, 2015.
[2] Z. Zhong, H. T. Qin, L. Liu, Y. B. Zhang, and M. G. Shan, “Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain,” *Opt. Exp.*, vol. 25, no. 6, pp. 6974–6982, 2017.
[3] L. S. Sui, M. T. Xin, and A. L. Tian, “Multiple-image encryption based on phase mask multiplexing in fractional Fourier transform domain,” *Opt. Lett.*, vol. 38, no. 11, pp. 1996–1998, 2013.
[4] Y. Wang and C. G. Quan, “Interference-based optical image encryption with silhouette removal by amplitude modulation,” *J. Opt.*, vol. 19, no. 10, 2017, Art. no. 105701.

[5] C. G. Zhang, B. N. Han, W. Q. He, X. Peng, and C. Xu, “A novel compressive optical encryption via single-pixel imaging,” *IEEE Photon. J.*, vol. 11, no. 4, pp. 1–8, Aug. 2019, Art. no. 7801208.

[6] H. Chen, C. Tanougast, Z. J. 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, 2017.

[7] X. J. Shen, C. Lin, and D. Z. Kong, “Fresnel-transform holographic encryption based on angular multiplexing and random-amplitude mask,” *Opt. Eng.*, vol. 51, no. 6, 2012, Art. no. 068201.

[8] M. H. Liao, W. Q. He, D. J. Lu, J. C. Wu, and X. Peng, “Security enhancement of the phase-shifting interferometry-based cryptosystem by independent random phase modulation in each exposure,” *Opt. Lasers Eng.*, vol. 89, pp. 34–39, 2017.

[9] Y. Qin, Z. P. Wang, Q. N. Pan, and Q. Gong, “Optical color-image encryption in the diffractive-imaging scheme,” *Opt. Lasers Eng.*, vol. 77, pp. 191–202, 2016.

[10] Y. Qin, Q. Gong, Z. P. Wang, and H. J. Wang, “Optical multiple-image encryption in diffractive-imaging-based scheme using spectral fusion and nonlinear operation,” *Opt. Exp.*, vol. 24, no. 23, pp. 26877–26886, 2016.

[11] W. Chen, X. D. Chen, and C. J. R. Sheppard, “Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain,” *Opt. Exp.*, vol. 20, no. 4, pp. 3853–3865, 2012.

[12] W. Chen, X. D. Chen, and C. J. R. Sheppard, “Optical image encryption based on diffractive imaging,” *Opt. Lett.*, vol. 35, no. 22, pp. 3817–3819, 2010.

[13] Y. S. Shi, T. Li, Y. L. Wang, Q. K. Gao, S. G. Zhang, and H. F. Li, “Optical image encryption via ptychography,” *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, 2013.

[14] P. Clemente, V. Duran, V. Torres-Company, E. Tajahuerce, and J. Lancis, ”Optical encryption based on computational ghost imaging,” *Opt. Lett.*, vol. 35, no. 14, pp. 2391–2393, 2010.

[15] W. Chen and X. D. Chen, “Ghost imaging for three-dimensional optical security,” *Appl. Phys. Lett.*, vol. 103, no. 22, 2013, Art. no. 221106.

[16] N. Rawat, I. C. Hwang, Y. Shi, and B. G. Lee, “Optical image encryption via photon-counting imaging and compressive sensing based ptychography,” *J. Opt.*, vol. 17, no. 6, 2015, Art. no. 065704.

[17] Y. Zhang and B. Wang, “Optical image encryption based on interference,” *Opt. Lett.*, vol. 33, no. 21, pp. 2443–2445, 2008.

[18] Y. Zhang, B. Wang, and Z. L. Dong, “Enhancement of image hiding by exchanging two phase masks,” *J. Opt. A-Pure Appl. Opt.*, vol. 11, no. 12, 2009, Art. no. 125406.

[19] P. Kumar, J. Joseph, and K. Singh, “Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator,” *Appl. Opt.*, vol. 50, no. 13, pp. 1805–1811, 2011.

[20] X. G. Wang and D. M. Zhao, “Optical image hiding with silhouette removal based on the optical interference principle,” *Appl. Opt.*, vol. 51, no. 6, pp. 686–691, 2012.

[21] W. Chen and X. D. Chen, “Security-enhanced interference-based optical image encryption,” *Opt. Commun.*, vol. 286, pp. 123–129, 2013.

[22] J. J. Cai, X. J. Shen, M. Lei, C. Lin, and S. F. Dou, “Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition,” *Opt. Lett.*, vol. 40, no. 4, pp. 475–478, 2015.

[23] J. J. Wu, W. Liu, Z. J. Liu, and S. T. Liu, “Cryptanalysis of an “asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition”,” *Appl. Opt.*, vol. 54, no. 30, pp. 8921–8924, 2015.

[24] Y. Wang, C. G. Quan, and C. J. Tay, “New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition,” *Appl. Opt.*, vol. 55, no. 4, pp. 679–686, 2016.

[25] J. J. Cai, X. J. Shen, and C. Lin, “Security-enhanced asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition,” *Opt. Commun.*, vol. 359, pp. 26–30, 2016.

[26] X. Y. Shi, Z. Y. Chen, D. M. Zhao, H. D. Mao, and L. F. Chen, “Phase retrieval encryption in an enhanced optical interference by key phase constraint,” *Appl. Opt.*, vol. 54, no. 11, pp. 3197–3203, 2015.

[27] W. Chen and X. D. 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, 2014.

[28] D. J. Lu, W. Q. He, M. H. Liao and X. Peng, “An interference-based optical authentication scheme using two phase-only masks with different diffraction distances,” *Opt. Laser Eng.*, vol. 89, pp. 40–46, 2017.

[29] S. P. Barfungpa and M. R. Abuturab, “Asymmetric cryptosystem using coherent superposition and equal modulus decomposition of fractional Fourier spectrum,” *Opt. Quant. Electron.*, vol. 48, no. 11, 2016, Art. no. 520.