Optica Applicata, Vol. LII, No. 4, 2022
DOI: 10.37190/oa220402

Optical asymmetric double-image encryption and authentication in an interference-based scheme using sparse representation

GUANGYU LUAN*, CAOJUN HUANG

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

*Corresponding author: luanguangyu@126.com

We report an optical asymmetric scheme for double-image encryption and authentication based on interference using sparse representation. We employ sparse representation and interference to process the Fresnel spectra related with the two original images, and then respectively acquire two ciphertexts and two pairs of private keys. Each original image possesses its corresponding two private keys. Furthermore, the decrypted image is compared with its corresponding plaintext with the aid of a nonlinear correlation for authentication. In the proposed scheme, any information concerning each primary image and comprising its silhouette cannot be recognized even though one, two, or even three masks of the two ciphertexts and two private keys are utilized for decryption. The Fresnel spectrum functions which have different diffraction distances enhance the security of the proposal significantly. Moreover, the proposal also avoids the crosstalk problem. The effectiveness and security of this proposed method are demonstrated via numerical simulations.

Keywords: optical encryption, asymmetry, interference, double-image, authentication.

1. Introduction

In recent decades, the use of optical encryption technologies [1−8] for image security has given rise to increased research attention on account of their unique physical characteristics, such as multiple parameters and high speed. As a representative technology, double random-phase encoding [9] was carried out in the Fourier transform domain. Afterwards, this technology further spreads to various other transform domains [10−14], such as the gyrator domain, Fresnel domain, and fractional Fourier domain. Meanwhile, image encryption approaches based on other optical technologies [15–25], such as digital holography, polarized light, diffractive imaging, iterative phase retrieval, and compressive sensing, have been also investigated for strengthening image security.

Interference-based encryption technology has offered a novel research perspective in optical encryption due to its non-iterative calculations and simplicity of use. Unfortunately, it has a drawback in the form of the silhouette problem [26]. That is, the silhouette information of the plaintext can leak out if any of two phase-only masks (POMs) is used in the decryption architecture. Subsequently, many approaches have been developed for silhouette removal. For instance, ZHONG *et al.* [27] presented a scheme that used discrete multiple-parameter fractional Fourier transform to produce three POMs for alleviating the silhouette problem. WANG and QUAN [28] achieved silhouette removal with the help of an amplitude modulation operation implemented on the original image. In particular, some results regarding multiple-image encryption based on interference have emerged. For instance, QIN *et al.* [29] encoded multiple primary images into POMs in the spatial domain. ZHANG *et al.* [30] combined the cascaded interference structure with the vector stochastic decomposition algorithm to devise a hierarchical method for multiple-image encryption. QIN and GONG [31] realized multiple-image encryption by utilizing interference and position multiplexing. However, owing to the crosstalk, the decrypted image had some degree of degradation in quality. Alternatively, some schemes [32,33] have been presented that use interference and multiplane phase retrieval algorithms. However, the iterative computations of their multiplane phase retrieval algorithms required considerable amounts of processing time. In addition, sparse representation technology [34,35]; *i.e.*, sparse sampling of the encrypted image, has been employed in image security authentication for extra protection. WANG *et al.* [36] integrated the sparse representations of plaintexts into an interim image using space multiplexing, and then encoded the interim image into two ciphertexts. However, this scheme still suffered from information leakage. Thus, despite great advancements, attaining high security levels of optical multiple-image encryption which makes use of the interference principle remains a major challenge.

We present a novel asymmetric approach of double-image encryption and authentication. The silhouette problem is thoroughly coped with two ciphertexts and two pairs of private keys. Compared with some previous methods that used interference, the crosstalk problem as well as time-consuming iterative calculations are non-existent in the proposal. Moreover, the Fresnel spectrum functions which employ different diffraction distances effectively enlarge the key space. And each of the two images has its own private keys and diffraction distance. The results of simulations confirm the reliability of the proposed double-image encryption and authentication scheme.

2. Scheme description

In our double-image encryption and authentication system, $f_1(x, y)$ and $f_2(x, y)$ represent the two original images. First, the novel complex value functions, $f_1(u, v)$ and $f_2(u, v)$, in the Fresnel domain are respectively created by employing $f_1(x, y)$ and $f_2(x, y)$, which can be expressed as

$$\begin{aligned} f_1(u, v) = {} & \mathrm{FrT}_{(-d_1, \lambda)}\left\{\sqrt{f_1(x, y)}\,\exp\left[i2\pi R_1^1(x, y)\right]\right\} \\ & + \mathrm{FrT}_{(-d_1, \lambda)}\left\{2R_1^2(x, y)\exp\left[i2\pi R_1^3(x, y)\right]\right\} \end{aligned} \tag{1}$$

$$f_2(u, v) = \mathrm{FrT}_{(-d_2,\,\lambda)}\left\{\sqrt{f_2(x, y)}\,\exp\left[i2\pi R_2^1(x, y)\right]\right\} + \mathrm{FrT}_{(-d_2,\,\lambda)}\left\{2R_2^2(x, y)\exp\left[i2\pi R_2^3(x, y)\right]\right\} \tag{2}$$

where $R_1^j(x, y)$ and $R_2^j(x, y)$ ($j = 1, 2, 3$) denote the random functions for original images 1 and 2, respectively, which generate a uniform distribution in the range [0, 1], $\mathrm{FrT}_{(-d_1,\,\lambda)}$ and $\mathrm{FrT}_{(-d_2,\,\lambda)}$ represent the Fresnel transforms, which having at propagation distances of d_1 and d_2 between the masks and the CCD plane, respectively, and the incident light wavelength λ.

Next, $f_k(u, v)$ ($k = 1, 2$) is multiplied by the binary amplitude mask $B_k(u, v)$ to acquire the sparse data $f_k^{\mathrm{s}}(u, v)$ as follows

$$f_k^{\mathrm{s}}(u, v) = f_k(u, v) \times B_k(u, v) \tag{3}$$

Here, $B_k(u, v)$ is randomly generated.

Then, $f_1^{\mathrm{s}}(u, v)$ and $f_2^{\mathrm{s}}(u, v)$ are added together to derive the synthesized function $\mathrm{SF}(u, v)$ as

$$\mathrm{SF}(u, v) = f_1^{\mathrm{s}}(u, v) + f_2^{\mathrm{s}}(u, v) \tag{4}$$

Another synthesized function $\mathrm{SF}^k(u, v)$ is constructed as

$$\mathrm{SF}^k(u, v) = -B_k(u, v)\,\mathrm{FrT}_{(-d_k,\,\lambda)}\left\{2R_k^2(x, y)\exp\left[i2\pi R_k^3(x, y)\right]\right\} - \sum_{j=1,\,\neq k}^{2} f_j^{\mathrm{s}}(u, v) \tag{5}$$

Thereafter, according to the interference principle, $\mathrm{SF}(u, v)$ and $\mathrm{SF}^k(u, v)$ are respectively encoded into two ciphertexts ($M_1(u', v')$ and $M_2(u', v')$) and two private keys ($M_3^k(u', v')$ and $M_4^k(u', v')$) as follows:

$$M_1(u', v') = \arg\left\{\mathrm{IFT}\left\{\frac{\mathrm{FT}\left[\mathrm{SF}(u, v)\right]}{\mathrm{FT}\left[h(u', v', d_3)\right]}\right\}\right\} - \arccos\left\{\frac{1}{2}\left|\mathrm{IFT}\left\{\frac{\mathrm{FT}\left[\mathrm{SF}(u, v)\right]}{\mathrm{FT}\left[h(u', v', d_3)\right]}\right\}\right|\right\} \tag{6}$$

$$M_2(u', v') = \arg\left\{\mathrm{IFT}\left\{\frac{\mathrm{FT}\left[\mathrm{SF}(u, v)\right]}{\mathrm{FT}\left[h(u', v', d_3)\right]}\right\} - \exp\left[iM_1(u', v')\right]\right\} \tag{7}$$

$$M_3^k(u', v') = \arg\left\{\mathrm{IFT}\left\{\frac{\mathrm{FT}\left[\mathrm{SF}^k(u, v)\right]}{\mathrm{FT}\left[h(u', v', d_4)\right]}\right\}\right\} - \arccos\left\{\frac{1}{2}\left|\mathrm{IFT}\left\{\frac{\mathrm{FT}\left[\mathrm{SF}^k(u, v)\right]}{\mathrm{FT}\left[h(u', v', d_4)\right]}\right\}\right|\right\} \tag{8}$$

$$M_4^k(u', v') = \arg\left\{\mathrm{IFT}\left\{\frac{\mathrm{FT}\left[\mathrm{SF}^k(u, v)\right]}{\mathrm{FT}\left[h(u', v', d_4)\right]}\right\} - \exp\left[iM_3^k(u', v')\right]\right\} \tag{9}$$

where

$$h(u', v', d_3) = \frac{\exp\left[i2\pi d_3/\lambda\right]}{id_3\lambda}\exp\left[\frac{i\pi(u'^2 + v'^2)}{d_3\lambda}\right]$$

$$h(u', v', d_4) = \frac{\exp\left[i2\pi d_4/\lambda\right]}{id_4\lambda}\exp\left[\frac{i\pi(u'^2 + v'^2)}{d_4\lambda}\right]$$

The two target images can be decrypted using the ciphertexts and private keys, which are located at predefined positions and illuminated by a coherent parallel light beam with a corresponding wavelength of λ, as shown in Fig. 1. The decryption process for $f_k(x, y)$ ($k = 1, 2$) can be deduced as

$$\begin{aligned} I_k^{\mathrm{s}}(x, y) &= \mathrm{FrT}_{(d_k,\,\lambda)}\Big\{\mathrm{FrT}_{(d_3,\,\lambda)}\left[M_1(u', v') + M_2(u', v')\right] \\ &\qquad + \mathrm{FrT}_{(d_4,\,\lambda)}\left[M_3^k(u', v') + M_4^k(u', v')\right]\Big\} \\ &= \mathrm{FrT}_{(d_k,\,\lambda)}\left\{B_k(u, v)\mathrm{FrT}_{(-d_k,\,\lambda)}\left\{\sqrt{f_k(x, y)}\,\exp\left[i2\pi R_k^1(x, y)\right]\right\}\right\} \end{aligned} \tag{10}$$

It can be ascertained from Eq. (10) that the decrypted result $I_k^{\mathrm{s}}(x, y)$ is a complex function concerning $f_k(x, y)$. In other words, the amplitude of recorded $I_k^{\mathrm{s}}(x, y)$ by a CCD camera (Fig. 1) is the partial information of $f_k(x, y)$. Obviously, the decrypted result of our method is immune to crosstalk noise. As shown in Fig. 1, authentication of the decrypted results is performed with a nonlinear correlation digitally processed on a computer.

Then, since $I_k^{\mathrm{s}}(x, y)$ with little information of $f_k(x, y)$ cannot be recognized by naked eyes, we employ a nonlinear correlation [36,37] to verify the presence of $f_k(x, y)$, and the correlation coefficient [38] to assess the quality of the decryption results. The non-

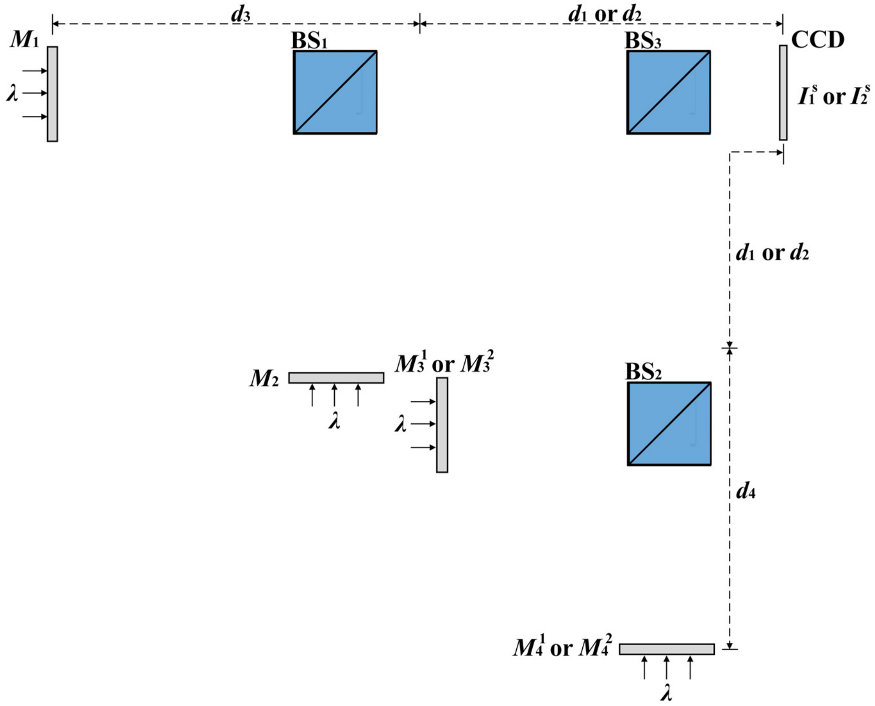

Fig. 1. Optical schematic architecture for decryption. BS: beam splitter; CCD: charge coupled device.

linear correlation and the correlation coefficient (CC) between the original image $f_k(x, y)$ and the decrypted image $I_k^{\mathrm{s}}(x, y)$ are respectively given as

$$\mathrm{NC}(x, y) = \mathrm{IFT}\left\{ \left| \mathrm{FT}\left[f_k(x, y) \right] \mathrm{FT}\left[I_k^{\mathrm{s}}(x, y) \right] \right|^{\omega - 1} \times \mathrm{FT}\left[f_k(x, y) \right] \mathrm{FT}\left[I_k^{\mathrm{s}}(x, y) \right] \right\} \tag{11}$$

$$\mathrm{CC} = \frac{E\left\{ f_k(x, y) - E\left[f_k(x, y) \right] \right\} \left\{ I_k^{\mathrm{s}}(x, y) - E\left[I_k^{\mathrm{s}}(x, y) \right] \right\}}{E\sqrt{\left\{ f_k(x, y) - E\left[f_k(x, y) \right] \right\}^2} \sqrt{\left\{ I_k^{\mathrm{s}}(x, y) - E\left[I_k^{\mathrm{s}}(x, y) \right] \right\}^2}} \tag{12}$$

where ω denotes the strength of the applied nonlinearity, and E denotes the expected value operator.

3. Simulation results and discussion

To demonstrate the effectiveness and robustness of our proposed method, we performed numerical simulations. In the simulations, the axial distances were set to $d_1 = 50$ mm,

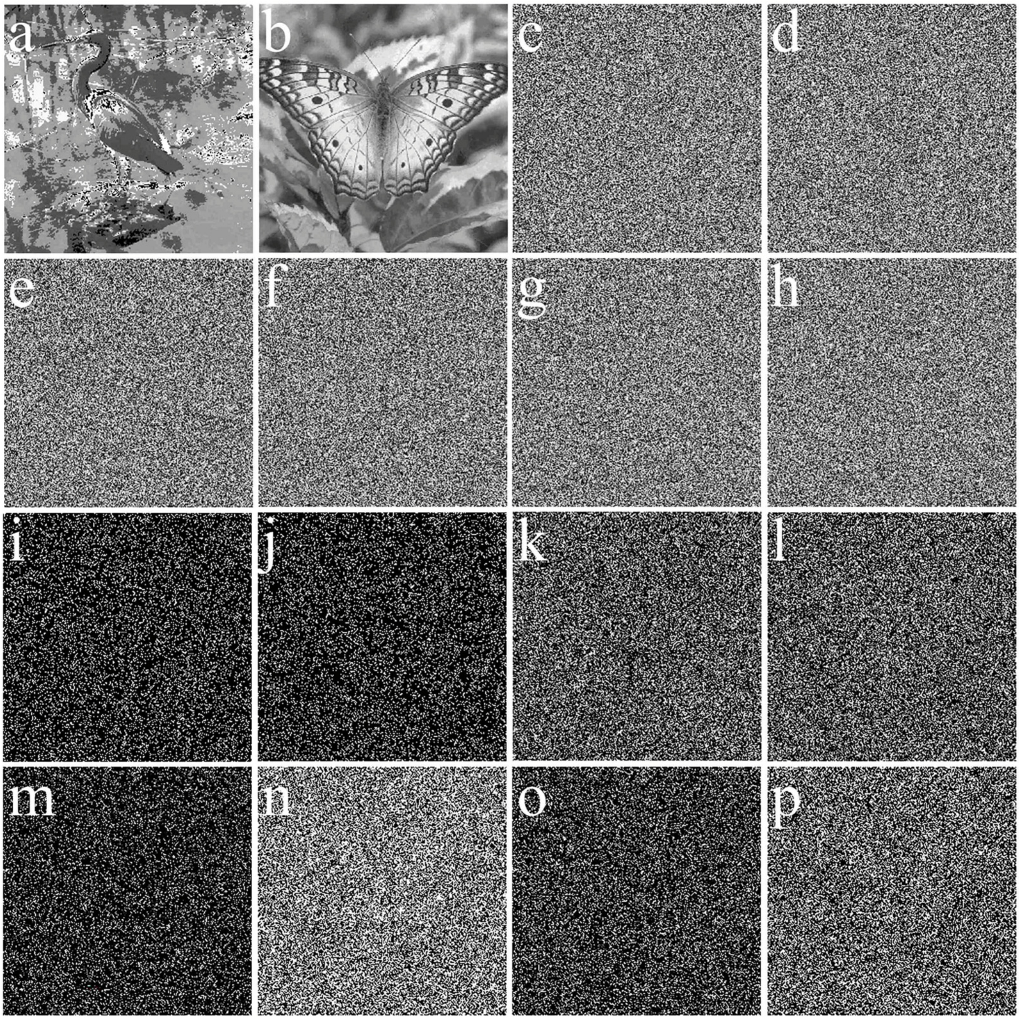

Fig. 2. (a–b) Two original images, (c–h) six public keys R_k^j, (i–j) two binary amplitude masks B_k, and (k–p) two ciphertexts and four private keys.

$d_2 = 75$ mm, $d_3 = 50$ mm, and $d_4 = 40$ mm, and the wavelength of the coherent parallel light beam was 633 nm. The two original images, the dimensions of each was 256 × × 256 pixels, are given in Figs. 2(a) and (b), and the six public keys, $R_k^j(x, y)$ ($k = 1, 2$ and $j = 1, 2, 3$), are given in Figs. 2(c)−(h). After we performed the Fresnel transform, we used the binary amplitude masks, $B_k(u, v)$ (16%), as shown in Figs. 2(i) and (j). Using the proposed approach and security keys, the ciphertexts ($M_1(u', v')$ and $M_2(u', v')$) and the private keys ($M_3^k(u', v')$ and $M_4^k(u', v')$) were obtained, as given in Figs. 2(k)−(p).

When all the correct keys and ciphertexts were used for decryption, we obtained recovered images, as displayed in Figs. 3(a) and (c). It is clear that information regard-

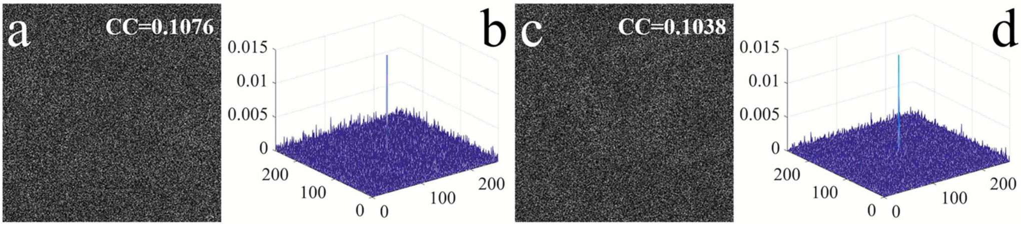

Fig. 3. (a) Decrypted image of Fig. 2(a) with M_1, M_2, M_3^1, and M_4^1. (b) Authentication result of (a). (c) Decrypted image of Fig. 2(b) with M_1, M_2, M_3^2, and M_4^2. (d) Authentication result of (c).

ing the original images could not be recognized using the naked eye owing to the use of the sparsification step. We then used a nonlinear correlation to authenticate the decrypted images (Figs. 3(a) and (c)), whose authentication results are shown in Figs. 3(b) and (d). It can be seen that there is one relatively prominent peak for each authentication distribution. Thus, the proposed approach can prove the presence and correctness of each of the hidden primary images.

To further demonstrate the performance of the proposed method, which does not suffer from the inherent silhouette problem of interference-based encryption, Figs. 4(a) to (h) give the nonlinear correlation results acquired using just one of M_1, M_2, M_3^1, M_3^2, M_4^1, and M_4^2; Figs. 5(a)–(l) give the nonlinear correlation results acquired using two of these parameters; and Figs. 6(a)–(h) give the nonlinear correlation results acquired when using three of the aforementioned parameters. It can be observed from Figs. 4–6 that one prominent peak is not produced in each of the authentication distributions. Thus, it can be concluded that the proposed approach does not suffer from the silhouette problem.

Moreover, to verify that the proposed method is very sensitive to the diffraction distance and illuminating wavelength, Figs. 7(a)–(c) give the nonlinear correlation outputs for axial distance d_1 errors of 0.2, 0.4, and 0.6 mm, respectively. Figures 8(a)

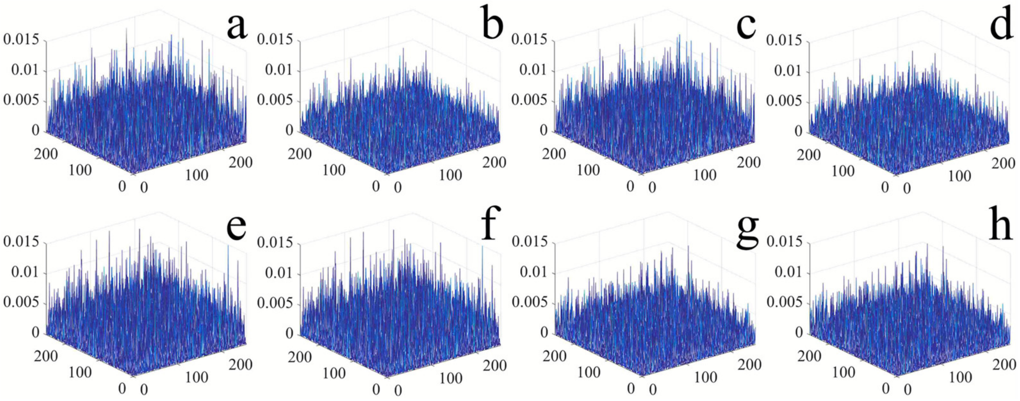

Fig. 4. Authentication results obtained with (a, b) M_1, (c, d) M_2, (e) M_3^1, (f) M_4^1, (g) M_3^2, and (h) M_4^2.

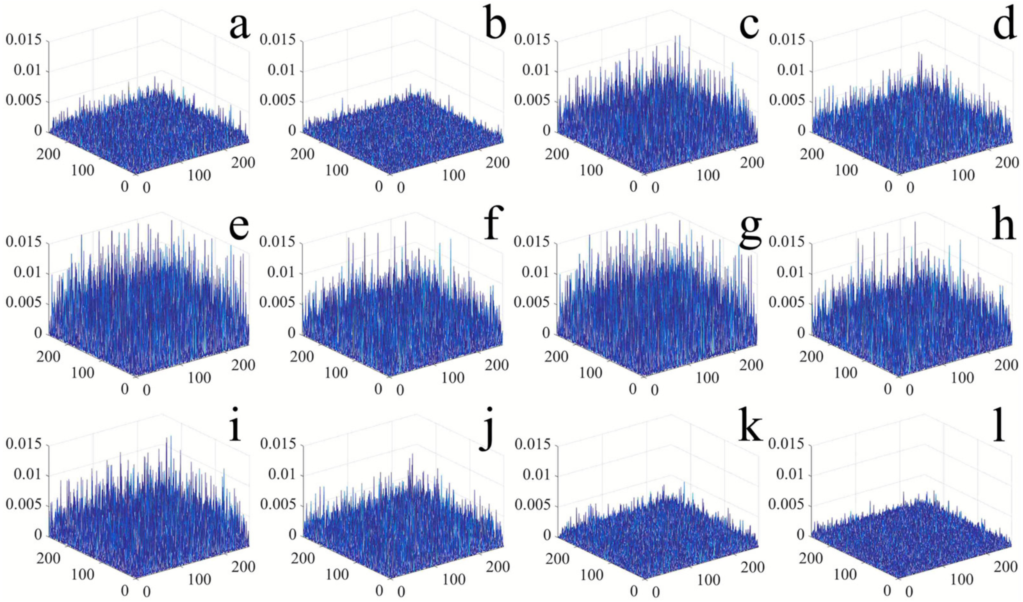

Fig. 5. Authentication results obtained with (a, b) M_1 and M_2, (c) M_1 and M_3^1, (d) M_1 and M_3^2, (e) M_1 and M_4^1, (f) M_1 and M_4^2, (g) M_2 and M_3^1, (h) M_2 and M_3^2, (i) M_2 and M_4^1, (j) M_2 and M_4^2, (k) M_3^1 and M_4^1, and (l) M_3^2 and M_4^2.

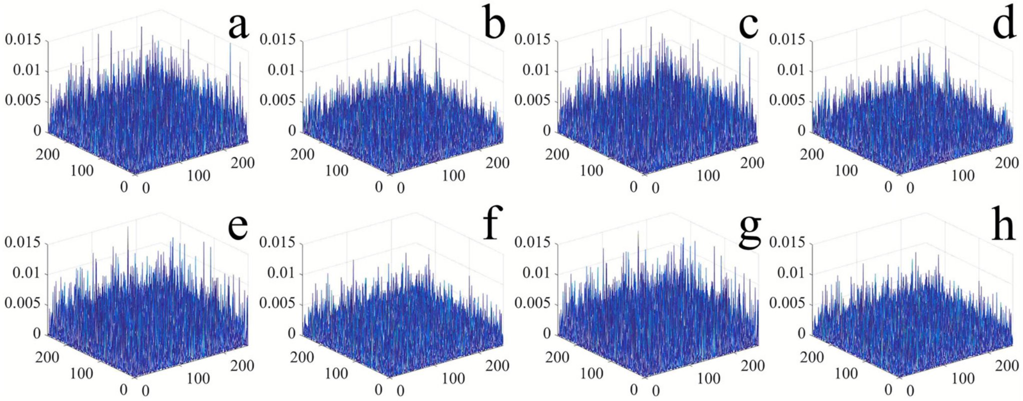

Fig. 6. Authentication results obtained with (a) M_1, M_2 and M_3^1, (b) M_1, M_2 and M_3^2, (c) M_1, M_2 and M_4^1, (d) M_1, M_2 and M_4^2, (e) M_1, M_3^1 and M_4^1, (f) M_1, M_3^2 and M_4^2, (g) M_2, M_3^1 and M_4^1, and (h) M_2, M_3^2 and M_4^2.

to (c) give the nonlinear correlation outputs for the same errors, respectively, and for axial distance d_2. It can be seen from Figs. 7 and 8 that some prominent peaks are produced in the nonlinear correlation output when the error of the axial distance, d_1 or d_2, is 0.4 and 0.6 mm. Next, Figs. 9(a) and (b) give the nonlinear correlation outputs for an error of 0.2 mm for axial distance d_3, and Figs. 9(c) and (d) give the nonlinear cor-

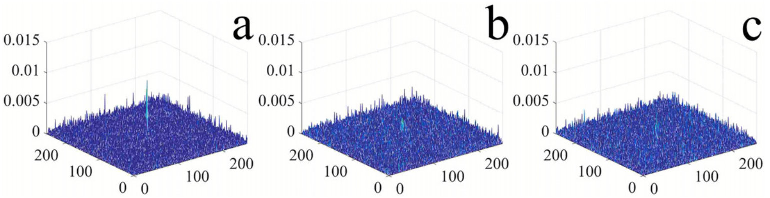

Fig. 7. Authentication results for deviations of (a) 0.2 mm, (b) 0.4 mm, and (c) 0.6 mm in diffraction distance d_1.

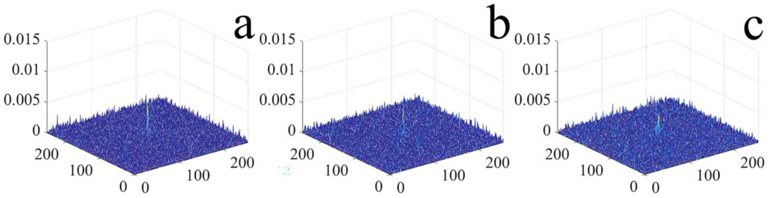

Fig. 8. Authentication results for deviations of (a) 0.2 mm, (b) 0.4 mm, and (c) 0.6 mm in diffraction distance d_2.

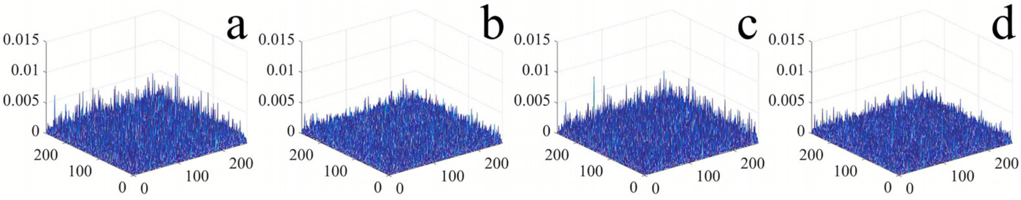

Fig. 9. Authentication results for a deviation of 0.2 mm in diffraction distance (a, b) d_3, and (c, d) d_4.

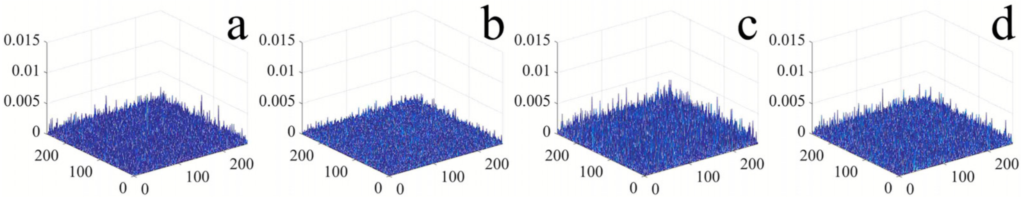

Fig. 10. Authentication results for deviations of (a, b) 1 nm, and (c, d) 2 nm in the wavelength.

relation outputs for the same error for axial distance d_4. Figures 10(a)–(d) give the nonlinear correlation outputs for errors of 1 and 2 nm in wavelength. These results reveal that a failure of the image authentication was caused along with a slight deviation of the diffraction distances or the illuminating wavelength.

In addition, we also evaluated the robustness of the proposed scheme against occlusion attacks and noise attacks. Figures 11(a) and (b) give ciphertexts with a 6% occlusion size, while Figs. 11(c) and (d) give the decrypted images of Figs. 11(a) and (b), and Figs. 11(e) and (f) give the nonlinear correlation outputs of Figs. 11(c) and (d).

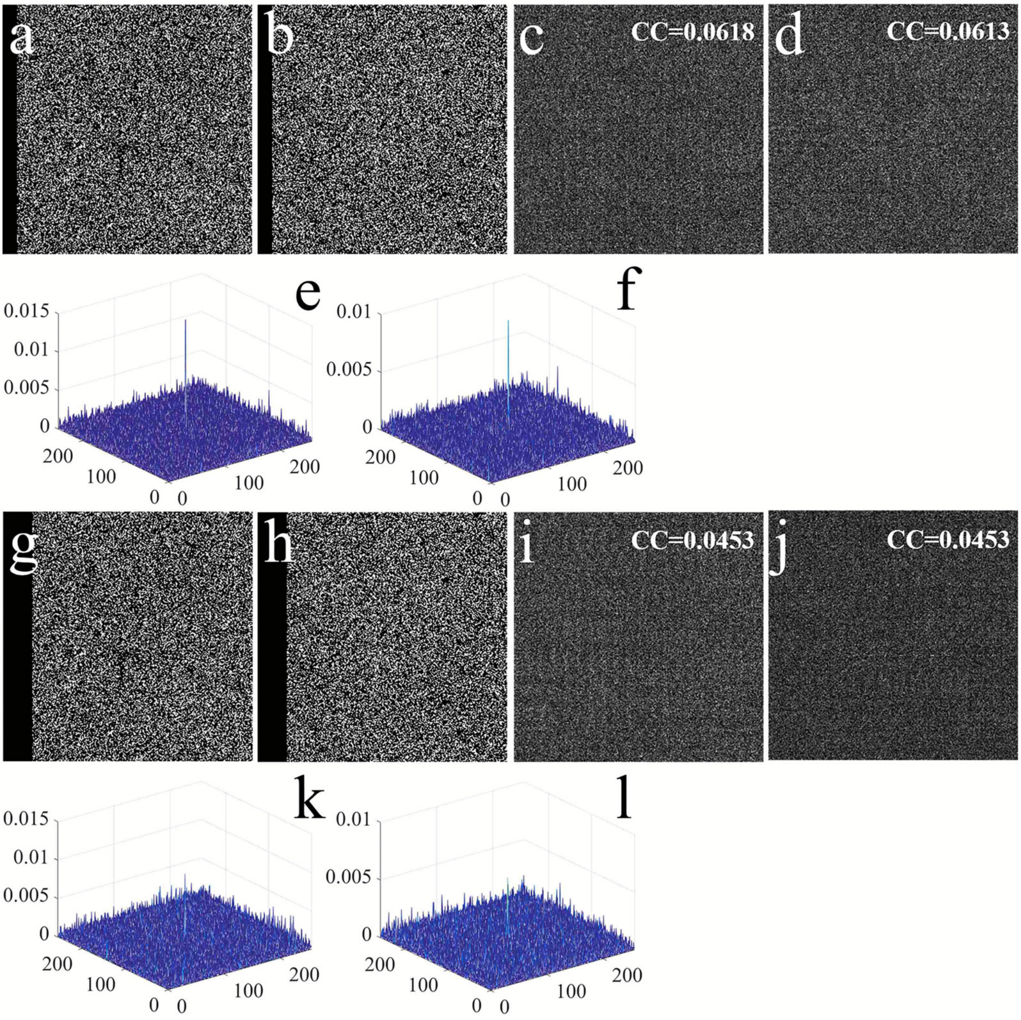

Fig. 11. (a, b) Ciphertexts with a 6% occlusion size, (c, d) decrypted images of (a) and (b), and (e, f) authentication results of (c) and (d). (g, h) Ciphertexts with a 12% occlusion size, (i, j) decrypted images of (g) and (h), and (k, l) authentication results of (i) and (j).

Next, Figs. 11(g) and (h) give ciphertexts with a 12% occlusion size; Figs. 11(i) and (j) give the decrypted images of Figs. 11(g) and (h), and Figs. 11(k) and (l) give the nonlinear correlation outputs of Figs. 11(i) and (j). Many correlation peaks appeared when the occlusion size was more than 12%. Figures 12(a) and (b) show decrypted images with zero-mean white additive Gaussian noise with a standard deviation of 0.01, and Figs. 12(c) and (d) show their respective nonlinear correlation outputs. Figures 12(e) and (f) show decrypted images with zero-mean white additive Gaussian noise with

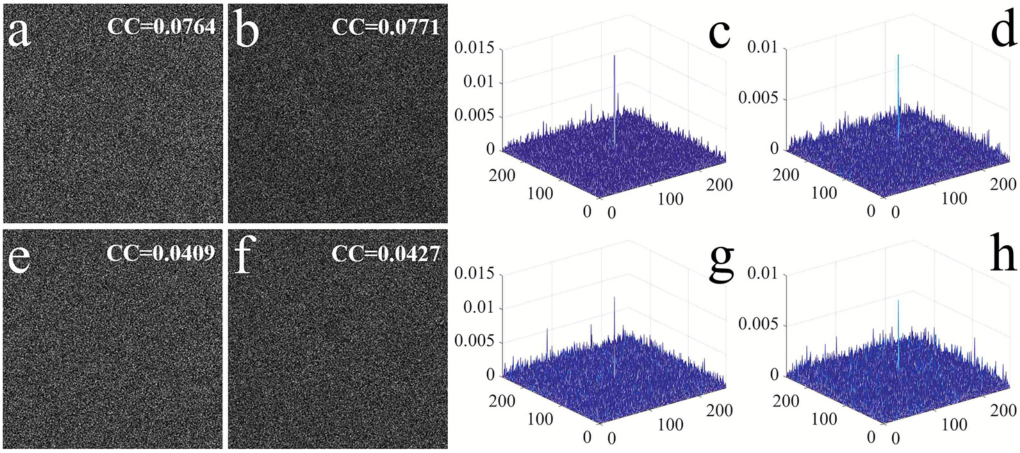

Fig. 12. (a, b) Decrypted images with zero-mean white additive Gaussian noise with a standard deviation 0.01, and (c, d) the authentication results of (a) and (b). (e, f) Decrypted images with zero-mean white additive Gaussian noise with a standard deviation 0.02, and (g, h) the authentication results of (e) and (f).

a standard deviation of 0.02; Figs. 12(g) and (h) respectively show their nonlinear correlation outputs. It is obvious from these results that there are nonlinear correlation prominent peaks. Thus, the proposed method has resistance to these attacks.

4. Conclusions

To conclude, we presented a new asymmetric double-image encryption and authentication scheme based on optical interference. Encouragingly, the silhouette problem is completely solved in the proposed scheme. The Fresnel spectrum functions which employ different diffraction distances improve the security level of our scheme. Each of the two images is decrypted by using its own private keys and diffraction distance. Relative to some previous methods that used interference, our proposed method not only avoid iterative calculations, but it also does not suffer from the crosstalk problem. In addition, it was demonstrated that our proposal is efficiently resistant to occlusion and noise attacks.

Acknowledgments
This work was supported by the Education Department Foundation of Heilongjiang Province of China (grant number 12541584) and Natural Science Foundation of Heilongjiang Province of China (grant number C2018050).

References

[1] Alfalou A., Brosseau C., *Recent advances in optical image processing*, Progress in Optics **60**, 2015, pp. 119–262, DOI: 10.1016/bs.po.2015.02.002.

[2] ALFALOU A., BROSSEAU C., *Optical image compression and encryption methods*, Advances in Optics and Photonics **1**(3), 2009, pp. 589–636, DOI: 10.1364/AOP.1.000589.

[3] CHEN W., JAVIDI B., CHEN X.D., *Advances in optical security systems*, Advances in Optics and Photonics **6**(2), 2014, pp. 120–155, DOI: 10.1364/AOP.6.000120.

[4] LUAN G.Y., ZHONG Z., SHAN M.G., *Optical multiple-image encryption in discrete multiple-parameter fractional Fourier transform scheme using complex encoding, theta modulation and spectral fusion*, Optica Applicata **51**(1), 2021, pp. 121–134, DOI: 10.37190/oa210110.

[5] SUI L.S., ZHAO X.Y., HUANG C.T., TIAN A.L., ANAND A., *An optical multiple-image authentication based on transport of intensity equation*, Optics and Lasers in Engineering **116**, 2019, pp. 116–124, DOI: 10.1016/j.optlaseng.2019.01.006.

[6] PEREZ-CABRE E., CHO M.J., JAVIDI B., *Information authentication using photon-counting double-random-phase encrypted images*, Optics Letters **36**(1), 2011, pp. 22–24, DOI: 10.1364/OL.36.000022.

[7] CARNICER A., MONTES-USATEGUI M., ARCOS S., JUVELLS I., *Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys*, Optics Letters **30**(13), 2005, pp. 1644–1646, DOI: 10.1364/OL.30.001644.

[8] PENG X., WEI H.Z., ZHANG P., *Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain*, Optics Letters **31**(22), 2006, pp. 3261–3263, DOI: 10.1364/OL.31.003261.

[9] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[10] RAJPUT S.K., NISHCHAL N.K., *Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform*, Applied Optics **52**(4), 2013, pp. 871–878, DOI: 10.1364/AO.52.000871.

[11] LI Y.B., ZHANG F., LI Y.C., TAO R., *Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform*, Optics and Lasers in Engineering **72**, 2015, pp. 18–25, DOI: 10.1016/j.optlaseng.2015.03.027.

[12] CHEN J.X., ZHU Z.L., LIU Z.J., FU C., ZHANG L.B., YU H., *A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains*, Optics Express **22**(6), 2014, pp. 7349–7361, DOI: 10.1364/OE.22.007349.

[13] ZHONG Z., ZHANG Y.J., SHAN M.G., WANG Y., ZHANG Y.B., XIE H., *Optical movie encryption based on a discrete multiple-parameter fractional Fourier transform*, Journal of Optics **16**(12), 2014, article no. 125404, DOI: 10.1088/2040-8978/16/12/125404.

[14] SUI L.S., DUAN K.K., LIANG J.L., HEI X.H., *Asymmetric double-image encryption based on cascaded discrete fractional random transform and logistic maps*, Optics Express **22**(9), 2014, pp. 10605–10621, DOI: 10.1364/OE.22.010605.

[15] CARNICER A., HASSANFIROOZI A., LATORRE-CARMONA P., HUANG Y.P., JAVIDI B., *Security authentication using phase-encoded nanoparticle structures and polarized light*, Optics Letters **40**(2), 2015, pp. 135–138, DOI: 10.1364/OL.40.000135.

[16] FATIMA A., NISHCHAL N.K., *Optical image security using Stokes polarimetry of spatially variant polarized beam*, Optics Communications **417**, 2018, pp. 30–36, DOI: 10.1016/j.optcom.2018.02.030.

[17] MALUENDA D., CARNICER A., MARTINEZ-HERRERO R., JUVELLS I., JAVIDI B., *Optical encryption using photon-counting polarimetric imaging*, Optics Express **23**(2), 2015, pp. 655–666, DOI: 10.1364/OE.23.000655.

[18] MOON I., YI F., HAN M., LEE J., *Efficient asymmetric image authentication schemes based on photon counting-double random phase encoding and RSA algorithms*, Applied Optics **55**(16), 2016, pp. 4328–4335, DOI: 10.1364/AO.55.004328.

[19] CHEN L.F., CHANG G.J., HE B.Y., MAO H.D., ZHAO D.M., *Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition*, Optics and Lasers in Engineering **88**, 2017, pp. 221–232, DOI: 10.1016/j.optlaseng.2016.08.013.

[20] SU Y.G., TANG C., CHEN X., LI B.Y., XU W.J., LEI Z.K., *Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map*, Optics and Lasers in Engineering **88**, 2017, pp. 20–27, DOI: 10.1016/j.optlaseng.2016.07.012.

[21] Li X.W., Xiao D., Wang Q.H., *Error-free holographic frames encryption with CA pixel-permutation encoding algorithm*, Optics and Lasers in Engineering **100**, 2018, pp. 200–207, DOI: 10.1016/j.optlaseng.2017.08.018.

[22] Chen Y., Liu Q., Wang J., Wang Q.H., *Single-channel optical encryption of color image using chessboard grating and diffraction imaging scheme*, Optical Engineering **56**(12), 2017, article no. 123106, DOI: 10.1117/1.OE.56.12.123106.

[23] Rawat N., Hwang I.C., Shi Y., Lee B.G., *Optical image encryption via photon-counting imaging and compressive sensing based ptychography*, Journal of Optics **17**(6), 2015, article no. 065704, DOI: 10.1088/2040-8978/17/6/065704.

[24] Wang Y., Quan C., Tay C.J., *Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm*, Optics and Lasers in Engineering **78**, 2016, pp. 8–16, DOI: 10.1016/j.optlaseng.2015.09.008.

[25] Qin Y., Wang Z.P., Wang H.J., Gong Q., Zhou N.R., *Robust information encryption diffractive -imaging-based scheme with special phase retrieval algorithm for a customized data container*, Optics and Lasers in Engineering **105**, 2018, pp. 118–124, DOI: 10.1016/j.optlaseng.2018.01.014.

[26] Zhang Y., Wang B., *Optical image encryption based on interference*, Optics Letters **33**(21), 2008, pp. 2443–2445, DOI: 10.1364/OL.33.002443.

[27] Zhong Z., Qin H.T., Liu L., Zhang Y.B., Shan M.G., *Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain*, Optics Express **25**(6), 2017, pp. 6974–6982, DOI: 10.1364/OE.25.006974.

[28] Wang Y., Quan C.G., *Interference-based optical image encryption with silhouette removal by amplitude modulation*, Journal of Optics **19**(10), 2017, article no. 105701, DOI: 10.1088/2040-8986/aa7e37.

[29] Qin Y., Jiang H.L., Gong Q., *Interference-based multiple-image encryption by phase-only mask multiplexing with high quality retrieved images*, Optics and Lasers in Engineering **62**, 2014, pp. 95 –102, DOI: 10.1016/j.optlaseng.2014.05.010.

[30] Zhang X., Meng X.F., Wang Y.R., Yang X.L., Yin Y.K., Li X.Y., Peng X., He W.Q., Dong G.Y., Chen H.Y., *Hierarchical multiple-image encryption based on the cascaded interference structure and vector stochastic decomposition algorithm*, Optics and Lasers in Engineering **107**, 2018, pp. 258 –264, DOI: 10.1016/j.optlaseng.2018.04.002.

[31] Qin Y., Gong Q., *Interference-based multiple-image encryption with silhouette removal by position multiplexing*, Applied Optics **52**(17), 2013, pp. 3987–3992, DOI: 10.1364/AO.52.003987.

[32] Chen W., Chen X.D., *Optical multiple-image encryption based on multiplane phase retrieval and interference*, Journal of Optics **13**(11), 2011, article no. 115401, DOI: 10.1088/2040-8978/13/11/115401.

[33] Shan M.G., Liu L., Liu B., Zhong Z., *Security-enhanced optical interference-based multiple-image encryption using a modified multiplane phase retrieval algorithm*, Optical Engineering **57**(8), 2018, article no. 083103, DOI: 10.1117/1.OE.57.8.083103.

[34] Chen W., Chen X.D., Stern A., Javidi B., *Phase-modulated optical system with sparse representation for information encoding and authentication*, IEEE Photonics Journal **5**(2), 2013, article no. 6900113, DOI: 10.1109/JPHOT.2013.2258144.

[35] Wang X.G., Zhou G.Q., Dai C.Q., *Optical double binary amplitude mask structure for security authentication*, IEEE Photonics Journal **8**(6), 2016, article no. 7805807, DOI: 10.1109/JPHOT.2016.2628798.

[36] Wang H.J., Qin Y., Huang Y.D., Wang Z.P., Zhang Y.Y., *Multiple-image encryption and authentication in interference-based scheme by aid of space multiplexing*, Optics and Laser Technology **95**, 2017, pp. 63–71, DOI: 10.1016/j.optlastec.2017.04.019.

[37] Gong Q., Liu X.Y., Li G.Q., Qin Y., *Multiple-image encryption and authentication with sparse representation by space multiplexing*, Applied Optics **52**(31), 2013, pp. 7486–7493, DOI: 10.1364/AO.52.007486.

[38] BARFUNGPA S.P., ABUTURAB M.R., *Asymmetric cryptosystem using coherent superposition and equal modulus decomposition of fractional Fourier spectrum*, Optical and Quantum Electronics **48**(11), 2016, article no. 520, DOI: 10.1007/s11082-016-0786-5.

Received June 15, 2021
in revised form January 11, 2022