

Three-dimensional image authentication using binarized images in double random phase integral imaging

Weitao Song (宋维涛)^{1,*}, Qijia Cheng (程齐家)¹, Yue Liu (刘越)^{2,3}, Yuanjin Zheng¹,
Zhiping Lin¹, and Yongtian Wang (王涌天)^{2,3}

¹*School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore*

²*Beijing Engineering Research Center of Mixed Reality and Advanced Display, School of Optics and Photonics, Beijing Institute of Technology, Beijing 100081, China*

³*AICFVE of Beijing Film Academy, Beijing 100088, China*

*Corresponding author: bitsongweitao@gmail.com

Received January 7, 2019; accepted March 1, 2019; posted online May 23, 2019

We proposed a three-dimensional (3D) image authentication method using binarized phase images in double random phase integral imaging (InI). Two-dimensional (2D) element images obtained from InI are encoded using a double random phase encryption (DRPE) algorithm. Only part of the phase information is used in the proposed method rather than using all of the amplitude and phase information, which can make the final data sparse and beneficial to data compression, storage, and transmission. Experimental results verified the method and successfully proved the developed 3D authentication process using a nonlinear cross correlation method.

OCIS codes: 100.4998, 110.6880.

doi: 10.3788/COL201917.051002.

Providing an efficient way to protect the authenticity of multimedia images, image authentication techniques are widely used in fields such as medical and access control^[1-5]. Among the current authentication schemes, encryption-based methods using optical encoding systems have become more popular due to the fast speed and multiple-dimensional characteristics.

Among these optical techniques for information security, double random phase encoding (DRPE)^[6] can be treated as one of the most widespread ones. DRPE can make an input image into a stationary white noise image using two random phase masks that are used to modulate the information in the spatial and Fourier domain, respectively. During the past three decades, the DRPE algorithm was also extended to Gyrator^[7], fractional Fourier^[8], and Fresnel domains^[9]. Moreover, many new techniques have been integrated with DRPE, such as ptychography^[10], aperture-key encoding^[11], and quick response codes^[12,13]. Researches also show that DRPE is vulnerable to some attacks, such as chosen-cipher text and known-plaintext attack^[14-18]. Some advanced methods, such as chaotic baker mapping^[19], compressive sensing, and space multiplexing^[20], are proposed to enhance the security of DRPE. With going deep into research gradually, data storage has been revealed as one problem. The encrypted information will occupy a large amount of memory, as the images from DRPE include both amplitude and phase information. That is not beneficial to data transmission during usage. Since DRPE was proposed, it has been extensively studied and many DRPE-related methods were presented to reduce the data size. The photon-counting technique^[21,22] was integrated with DRPE to achieve image authentication with a sparse image. Moreover, the decrypted image cannot be visually recognized but can be successfully authenticated with

a nonlinear cross correlation method when the number of photons is low. However, DRPE with photon-counting techniques still needs a complex-valued wave front in the sensor, which would also make the system complicated. Fortunately, researchers have proved that phase information is the main part for a successful image authentication. Thus, some methods based on the phase part of encrypted images are presented. It was also shown that partial phase information along with the nonlinear cross correlation algorithm can achieve successful image authentication^[23,24]. In these methods, only part of the phase data is required and the decrypted images can be recognized using the nonlinear cross correlation algorithm even when they cannot be recognized by human eyes. That is, partial phase information introduces the nonlinear property into the system and makes its security enhanced.

Most of the previous image authentication methods are based on two-dimensional (2D) image data, while three-dimensional (3D) information has been found useful in many fields. Integral imaging (InI) has received significant attentions and been applied in depth acquisition, naked-eye displays, near-eye displays, tracking, and recognition since it was proposed by Lippmann^[25-28]. This promising imaging technique can also be used in image authentication, which can provide 3D information^[29,30]. The photon-counting technique^[31] and partial phase information^[32] were employed by combining with InI and DRPE for the 3D image authentication. Even though these methods can fulfil 3D image authentication and have reduced the storage of encrypted data, they still need a lot of resources for data storage and transmission because there are a series of 2D elemental images in InI. Furthermore, the encrypted image with phase or amplitude format is not good for information hiding or watermarking.

In this Letter, a 3D image authentication method is presented with binary images that can rapidly reduce the size of the final data and is beneficial to information storage. In this method, a bunch of 2D elemental images is recorded by the InI method and then encrypted with the DRPE algorithm. Partial phase images are used in the final data, and the reconstructed 3D object is successfully authenticated with the sparse data using computational reconstruction, the DRPE algorithm, and the nonlinear cross correlation algorithm sequentially.

Figure 1 provides the procedure of the proposed 3D image authentication method, which is divided into the encryption and decryption parts. The 3D scene is firstly captured and recorded as 2D elemental images by the InI system, which is shown in Fig. 2(a). Multiple sensors can record the light emanating from the 3D scene. Each sensor captures a 2D elemental image of a specific perspective, which contains the directional information of the 3D scene. The sensors in this type of InI system can be placed in a flexible plane and, therefore, do not require the optical axis of each sensor to be parallel. During the construction process, each elemental image is back-projected onto the corresponding reconstruction depth and is then overlapped with the other back-projected elemental images, which are shown in Fig. 2(b). The relationship between the reconstruction coordination and the sensor coordination should be obtained in advance. The value of each pixel in the final depth images will be the average

of all the corresponding pixel values from all the elemental images. This record and the reconstruction procedure have already been discussed by sequential or parallel computing in detail in previous works^[33].

These 2D elemental images include target information from different directions. The DRPE algorithm is applied to encrypt these elemental images to make the data safe during the transmission process. As mentioned above, DRPE can be implemented in the Fourier, Fresnel, Gyrator, and fractional Fourier domains. Here, to make it simple, DRPE with the Fourier domain was employed. In DRPE, the input image is first modulated by a random mask $R_1(x, y)$ in the spatial domain. Then, the modulated image is propagated through a Fourier lens and further modulated by another random phase mask $R_2(x, y)$ in the Fourier domain. These two random masks can be expressed as $\exp[j2\pi r_1(x, y)]$ and $\exp[j2\pi r_2(\mu, \nu)]$, where $r_1(x, y)$ and $r_2(\mu, \nu)$ are uniformly distributed over $(0, 1)$. The encrypted image $E(x, y)$ of input image $I(x, y)$ can be given by two times of the 2D Fourier transform. The encrypted images consist of amplitude and phase parts due to the complex format. To reduce the size of encrypted data, only the phase part is obtained by discarding all of the amplitude part, and then the images used for image authentication are given by quantifying the phase images into binary images $B(x, y)$. Here, during the binarization process, all phase values less than zero are set to be zero, while others are one, which can be expressed by a step function:

$$\begin{aligned} B(x, y) &= \chi_A[E(x, y)] \\ &= \chi_A\{\zeta^{-1}\{\zeta\{I(x, y) \exp[j2\pi r_1(x, y)]\} \\ &\quad \times \exp[j2\pi r_2(\mu, \nu)]\}\}, \end{aligned} \quad (1)$$

where ζ and ζ^{-1} denote a 2D Fourier transform and inverse 2D Fourier transform, respectively. The step function is given as

$$\chi_A(x) = \begin{cases} 1, & x > 0 \\ 0, & x \leq 0 \end{cases}. \quad (2)$$

In this case, all of the encrypted 2D images become 2D binary images, and it is greatly beneficial to the data compression, storage, transmission, and hiding.

In terms of the decryption process (also shown in Fig. 1), a group of binary elemental images is given to be authenticated, which may be the true class (if they contain the correct information of the reference 3D scene). To authenticate the given group, these binary images are firstly converted into phase images $R(x, y)$ by setting 0 values as $-\pi$ and 1 values as π :

$$R(x, y) = 2\pi B(x, y) - \pi. \quad (3)$$

In this step, the original phase images cannot be totally recovered, and only partial phase information is obtained. Then, the DRPE algorithm is applied to these recovered

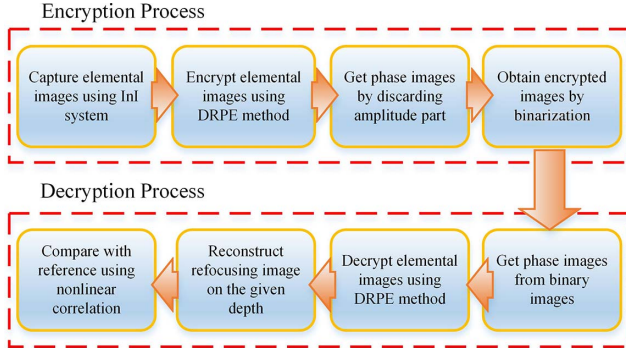


Fig. 1. Schematic diagram of the proposed image authentication system.

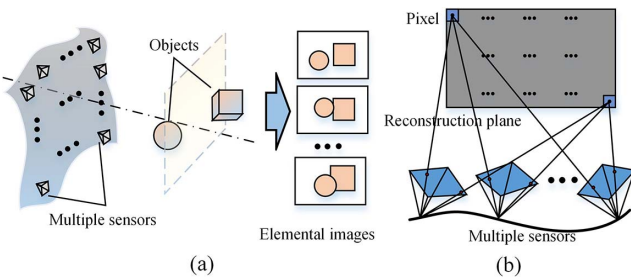


Fig. 2. Schematic diagram of integral imaging. (a) Integral imaging capture system. (b) Digital reconstruction process.

2D elemental phase images, which will be an inverse process of DRPE encryption. Since the first random mask used in the encryption step does not alter the intensity of the decrypted image with modulus calculation, it can be excluded to obtain the decrypted image $D(x, y)$. $|\cdot|$ is the modulus operation, and $*$ denotes the complex conjugate:

$$D(x, y) = |\zeta\{\zeta^{-1}[R(x, y)]\{\exp[j2\pi r_2(\mu, v)]\}^*\}|. \quad (4)$$

Since the phase images only contain some original phase information, the decrypted 2D elemental images cannot reveal all of the target information. Thus, it will not easily be recognized by the naked eye. The depth images or digital refocusing images can be reconstructed at a given distance using the reconstruction algorithm, as mentioned above.

The depth images can be authenticated using a nonlinear cross correlation transform method, which is widely applied for image authentication and recognition. The nonlinear cross correlation transform method can achieve a better correlation peak for true class images when compared with other correlation methods, even for eye-unrecognized images. The nonlinear correlation transform $NC(x, y)$ between two images $T_1(x, y)$ and $T_2(x, y)$ can be mathematically represented as the following equation, which has been applied in Refs. [23,32]:

$$NC = |\zeta^{-1}\{\zeta[T_1(x, y)]\{\zeta[T_1(x, y)]\}^* \times |\zeta[T_2(x, y)]\{\zeta[T_2(x, y)]\}^{*k-1}\}|. \quad (5)$$

Usually, the nonlinear correlation plane will have a remarkable high peak for true class images, and it is a noise-like distribution or very wide peak for a false class image. Here, parameter k is the strength of the applied nonlinearity, which can be evaluated by the best peak-to-correlation energy (PCE) result for different cases. The resolution of the analyzed image is $M \times N$, and PCE can be given as^[23,32]

$$PCE = \max[NC(x, y)] \left/ \sum_{x,y=1}^{M,N} NC(x, y) \right|. \quad (6)$$

To verify this method, an experiment was set up. Two toys were used as 3D objects that are captured by an InI system, and the InI system is shown in Fig. 3(a). The experiment given in this Letter was based on grayscale images. In terms of color images with red, green, and blue (RGB) channels or multispectral channels, the presented method should be firstly applied in the images for each channel, and then the results can be merged into the final color images. 10×10 elemental images were obtained by moving the camera on one plane facing the toys, which was controlled by a guide rail with a stepper motor. The disparity between any two adjacent viewpoints (movement step) was 2.5 cm, and the distance between the 3D target and camera plane was set as 50 cm. In fact, the viewpoints in InI can be arbitrary or on a flexible

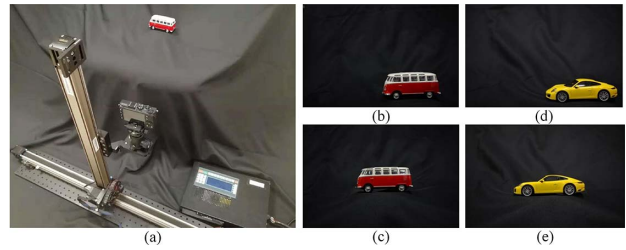


Fig. 3. Experimental set up and some of the elemental images for true and false classes. (a) Experimental set up. (b), (c) Elemental images from the true class. (d), (e) Elemental images from the false class.

plane, as mentioned above, but it is convenient to place these viewpoints on one plane with the same pitch. In this experiment, one toy bus was used as a true class and the other toy car as false class image for the verification of the 3D image authentication algorithm. The size of each elemental image was resized into 245×375 , and some of the elemental images obtained by this InI system are shown in Fig. 3, where Figs. 3(b) and 3(c) are used as true class and Figs. 3(d) and 3(e) as false class images.

As mentioned above, these 10×10 elemental images from the InI system were then encrypted by the DRPE algorithm. Taking one image from the group as an example, the encrypted elemental images, which consist of amplitude and phase parts from the DRPE, are shown in Fig. 4. Figures 4(a) and 4(b) are the images corresponding to the elemental image [Fig. 3(b)] in the true class, and Figs. 4(c) and 4(d) are the encrypted ones for the false class. It is noted that the encrypted images have a noise-like distribution and cannot reveal any information in the original images. The complex format will increase the size of the original elemental images. We discarded all of the amplitude information and only use the phase part in the encrypted images, which still needs a lot of space to handle these phase images due to the number of elemental images in a 3D InI system. These phase images were finally quantified into a binary image by setting the phase value less than zero as zero and others as one

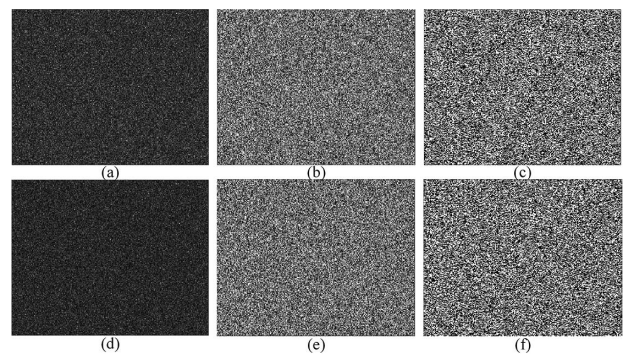


Fig. 4. (a) Amplitude, (b) phase, and (c) binary images of the encrypted elemental image from DRPE for the true class. (d) Amplitude, (e) phase, and (f) binary images of the encrypted elemental image from DRPE for the false class.

where the original phase value in the encrypted images ranges from $-\pi$ to π . Consequently, the quantified binary images are very sparse and greatly beneficial to data compression, storage, and transmission. In addition, it would be much easier to hide these binary images using some image watermarking or hiding techniques. Two of the quantified binary images from encrypted elemental images are given in Figs. 4(c) and 4(f), which correspond to the elemental images in the true and false classes, respectively.

In terms of the authentication process, the receiver gets the binary images, and these images may be from the true class or false class. Thus, to verify the process, binary images from both classes acted as input images, which were obtained above (Fig. 4). To conduct the final image authentication, the quantified binary images are converted into phase images by setting zero values as $-\pi$ and others as π . These recovered phase images are decrypted using the two correct random phase keys in the DRPE algorithm. The decrypted elemental images from the phase image recovered from input binary images for true and false classes are shown in Figs. 5(a) and 5(d), respectively (taking one image from either class as an example). Moreover, the corresponding decrypted elemental images using all information including amplitude and phase are also given in Figs. 5(b) and 5(e) for comparison. It is noted that the target in the decrypted elemental images from quantified binary images is not visually recognized, while it is much easier to tell the object in the decrypted image that is obtained from all encryption information. The property of visually unrecognized targets in decrypted 2D elemental images can enhance the image authentication system in another layer because it can distract the attacker's attention. These decrypted elemental images are employed to reconstruct the depth image using the computational reconstruction method mentioned above. The reconstructed depth images from the true and false classes at the reconstruction depth are shown in Figs. 5(c) and 5(f). It is found that the target in the reconstructed image is much better than that in the decrypted elemental images, because each elemental

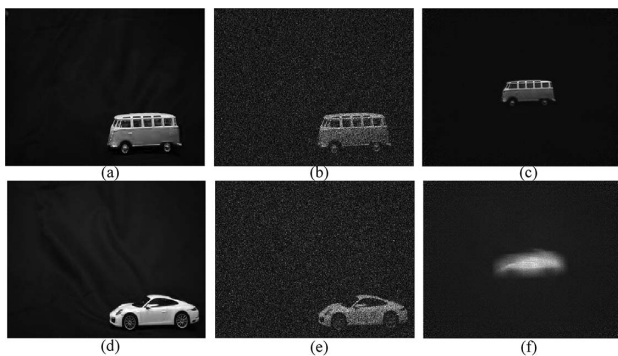


Fig. 5. (a) Original, (b) decrypted elemental images, and (c) reconstructed 3D image of the true class. (d) Original, (e) decrypted elemental images, and (f) reconstructed 3D image of the false class.

image can contribute information for the reconstruction of the depth image.

The 3D depth images and 2D elemental images can be successfully authenticated using the nonlinear cross correlation methods. The nonlinear correlation planes for true and false classes based on 3D and 2D information are shown in Fig. 6. For 3D image authentication, the depth image reconstructed from the true decrypted elemental images was used as the reference image, while the first elemental image of true class was treated as the reference one in 2D image authentication. Both the 2D and 3D images can be authenticated using the nonlinear correlation algorithm for true and false classes, which can be verified from Fig. 6. A high narrow peak in the center of the nonlinear correlation plane can be found when using true images, while the correlation plane has a noise-like distribution for the false class. In addition, the peak in the nonlinear correlation plane for the 3D image is higher and narrower than that of the 2D image for the true class image, which means information in each decrypted elemental image can be helpful for the final 3D image authentication in the InI system.

In the process using nonlinear cross correlation, 0.1 was chosen as the value of parameter k for the image authentication calculation, which is estimated from the simulation results. The value of k was varied from 0 to 0.9 with intervals of 0.1 to measure the corresponding PCE for the 2D and 3D image authentication for both true and false classes. The true and false class images can be differentiated for both 2D and 3D image authentication within a range of k , which is shown in Fig. 7. It is noted that the best PCE value can be achieved with the k value of 0.3 for the 2D image authentication, and k is better when set as 0.3 for the 3D image authentication. Therefore, 0.3 can be chosen as the final k value in the

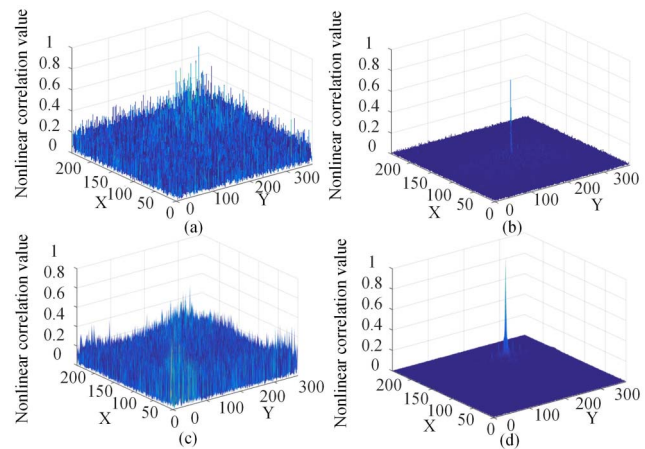


Fig. 6. (a), (c) Nonlinear correlation planes for the reconstructed 3D image and decrypted 2D elemental image of false class targets. (b), (d) Nonlinear correlation planes for the reconstructed 3D image and decrypted 2D elemental image of true class images.

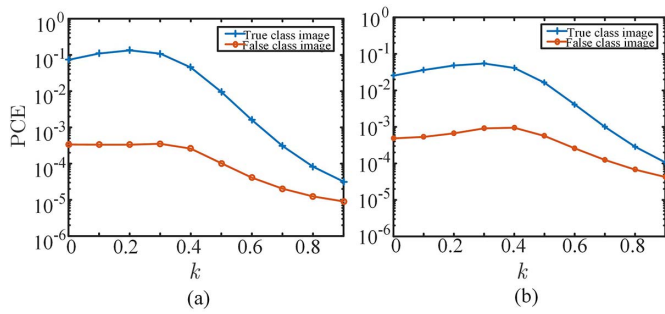


Fig. 7. PCE results for (a) 2D and (b) 3D images with varied k values.

nonlinear correlation equation to get the best result in the proposed 3D authentication method.

In this Letter, a 3D image authentication method using binarized images in double random phase InI was presented and verified. Compared with the traditional image authentication methods, the presented approach will decrease the data volume greatly. When taking the eight-bit grayscale images as an example, the data of binary images will be reduced to one eighth of that of the previous method, which will be beneficial to data compression, transmission, and storage, especially when applied in information hiding or watermarking. The authentication method may not work well in the InI system, where the elemental images are captured in scenarios of low light or a scattering medium^[22,31,34]. Because the elemental image may lose too much information to achieve a successful authentication after binary quantization, future works include applying this method in these scenarios.

This work was supported by the National Key Research and Development Program of China (No. 2018YFB1005002), the National Natural Science Foundation of China (No. 61727808), and the National Research Foundation of Singapore (No. NRF-CRP11-2012-01).

References

1. A. Haouzia and R. Noumeir, *Multimedia Tools Appl.* **39**, 1 (2008).
2. A. Alfalou and C. Brosseau, *Adv. Opt. Photon.* **1**, 589 (2009).
3. R. Thabit and B. E. Khoo, *Multimedia Tools Appl.* **76**, 309 (2017).
4. H. Zhao, J. Liu, J. Jia, N. Zhu, J. Xie, and Y. Wang, *Opt. Commun.* **286**, 85 (2013).
5. W. Chen, B. Javidi, and X. Chen, *Adv. Opt. Photon.* **6**, 120 (2014).
6. P. Refregier and B. Javidi, *Opt. Lett.* **20**, 767 (1995).
7. G. Situ and J. Zhang, *Opt. Lett.* **29**, 1584 (2004).
8. J. Chen, Z. L. Zhu, C. Fu, L. B. Zhang, and Y. Zhang, *Optik* **136**, 1 (2017).
9. Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, *Opt. Express* **18**, 12033 (2010).
10. Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, *Opt. Lett.* **38**, 1425 (2013).
11. X. Wang, W. Chen, and X. Chen, *Opt. Express* **22**, 28077 (2014).
12. A. Markman, J. Wang, and B. Javidi, *Optica* **1**, 332 (2014).
13. W. Chen, X. Wang, and X. Chen, *Opt. Express* **23**, 6239 (2015).
14. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, *Opt. Lett.* **30**, 1644 (2005).
15. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, *Opt. Express* **14**, 3181 (2006).
16. G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, *Appl. Opt.* **46**, 5257 (2007).
17. G. Li, W. Yang, D. Li, and G. Situ, *Opt. Express* **25**, 8690 (2017).
18. Q. Wang, A. Alfalou, and C. Brosseau, in *Frontiers in Optics* (2017), paper JTu2A.96.
19. A. M. Elshamy, A. N. Z. Rashed, A. E.-N. A. Mohamed, O. S. Faragalla, Y. Mu, S. A. Alshebeili, and F. E. Abd El-Samie, *J. Lightwave Technol.* **31**, 2533 (2013).
20. B. Deepan, C. Quan, Y. Wang, and C. J. Tay, *Appl. Opt.* **53**, 4539 (2014).
21. E. A. Watson and G. M. Morris, *Appl. Opt.* **31**, 4751 (1992).
22. S. Yeom, B. Javidi, and E. Watson, *Opt. Express* **13**, 9310 (2005).
23. W. Chen and X. Chen, *J. Opt.* **16**, 218 (2014).
24. W. Chen, X. Chen, A. Stern, and B. Javidi, *IEEE Photon. J.* **5**, 6900113 (2013).
25. W. Song, Y. Wang, D. Cheng, and Y. Liu, *Chin. Opt. Lett.* **12**, 060010 (2014).
26. A. Stern and B. Javidi, *Proc. IEEE* **94**, 591 (2006).
27. X. Yu, X. Sang, X. Gao, S. Yang, B. Liu, D. Chen, B. Yan, and C. Yu, *Chin. Opt. Lett.* **16**, 041001 (2018).
28. C. T. Seo, S. W. Kang, and M. Cho, *Chin. Opt. Lett.* **15**, 081102 (2017).
29. X. Li, Q. H. Wang, S. T. Kim, and I. K. Lee, *Opt. Commun.* **381**, 260 (2016).
30. X. Li, M. Zhao, Y. Xing, L. Li, S. T. Kim, X. Zhou, and Q.-H. Wang, *Opt. Express* **25**, 31516 (2017).
31. M. Cho and B. Javidi, *Opt. Lett.* **38**, 3198 (2013).
32. F. Yi, Y. Jeoung, and I. Moon, *Appl. Opt.* **56**, 4381 (2017).
33. W. Song, D. Weng, Y. Liu, and Y. Wang, in *Digital Holography and Three-Dimensional Imaging* (2017), paper W2A.7.
34. Y. Lee and H. Yoo, *Opt. Lasers Eng.* **77**, 31 (2006).