Research Article | Vol. 29, No. 16 / 2 August 2021 / Optics Express 25675
Optics EXPRESS

Optical hiding based on single-input multiple-output and binary amplitude-only holograms via the modified Gerchberg-Saxton algorithm

LINA ZHOU,[1] YIN XIAO,[1] ZILAN PAN,[1] YONGGUI CAO,[1] AND WEN CHEN[1,2,*]

[1]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China
[2]The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen 518057, China
*owen.chen@polyu.edu.hk

Abstract: Optics has provided a promising means for the development of information hiding in recent years. However, conventional optical information hiding systems can only hide a limited number of images, and optical implementation complexity is usually high in conventional methods. In this paper, we propose a new scheme to implement optical information hiding based on single-input multiple-output (SIMO) and binary amplitude-only holograms (AOHs) using the modified Gerchberg-Saxton algorithm (MGSA). Different from conventional optical hiding methods with the limited multiplexing capacity, the proposed scheme can retrieve a large number of different secret images from one single host image during optical retrieval. In addition, it is also illustrated that optical implementation complexity is reduced in the proposed method. Simulations and optical experiments are conducted to verify feasibility, security and robustness of the proposed method. It is expected that the proposed method could open up a different research perspective for optical multiple-image hiding.

© 2021 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

1. Introduction

In recent years, we have witnessed a great stride made in optical technologies and their applications in the field of optical security for data transmission and data storage [1–4]. Optical encryption and hiding usher in a new era of information security, which promotes the evolution of cryptography and steganography. The prevalence of optical means widely applied for cryptography and steganography can be ascribed to its major properties, i.e., parallel processing and intrinsic parameters of optical setups (e.g., amplitude, phase, polarization and wavelength) [2–4]. Double random phase encoding (DRPE) [5] was the first optical method implemented by using two random phase-only masks respectively located at the input plane and the Fourier plane. Over the decades, DRPE scheme has been developed and extended to various domains, e.g., Fresnel domain, Gyrator domain and fractional Fourier domain [6–8]. Many studies related to optical cryptography and steganography have also been conducted based on computational ghost imaging, computer-generated hologram, diffractive imaging and other optical techniques [1–4,9–12].

The optical technologies aforementioned are usually applied to optical single-image encoding and hiding, which are inadequate for the coming age of data explosion. To meet the requirement of large-data hiding and transmission, optical multiple-image encoding and hiding have to be studied [13–20]. In a comparison with optical single-image hiding, optical multiple-image hiding conceal some different secret images into a host image, which overcomes the challenges existing in data storage and data transmission. Current optical multiple-image hiding schemes originate from multiplexing techniques. Multiplexing provides the possibility to store big data on a single crystal, and massive hiding strategies have been developed attributing to sensitivity to various optical

#428564 https://doi.org/10.1364/OE.428564
Journal © 2021 Received 21 Apr 2021; revised 26 Jun 2021; accepted 1 Jul 2021; published 27 Jul 2021

Optics EXPRESS

parameters. Similarly, optical multiplexing was proposed to implement optical multiple-image encoding and hiding by exploiting sensitiveness of optical parameters [13–20]. Over the past decades, optical multiple-image encoding and hiding have drawn great attention owing to some striking properties, e.g., the enlarged hiding capacity, facile transmission and effective storage etc. For the multiplexing, information of secret images is superposed to generate a host image, and then each secret image can be retrieved from the host image by using its corresponding optical keys or parameters. For instance, wavelength multiplexing was proposed for optical multiple-image encoding, in which different images can be retrieved by using the corresponding wavelengths. Similarly, position multiplexing, polarization multiplexing, spectral multiplexing, angular multiplexing, aperture modulation and theta modulation based multiple-image encoding and hiding have been developed by using the intrinsic properties of optical techniques [14–20]. However, these multiplexing strategies are restricted by optical calibration problems and the limited number of secret images to be hidden. In addition, optical multiple-image encoding and hiding have also been reported by using iterative phase retrieval algorithms [6,18]. However, these iterative algorithms are usually complex and time-consuming, and the hiding capacity is still limited. Hence, traditional optical multiple-image hiding methods suffer from a limited number of secret images to be processed, difficult calibration of optical setups and the relatively complicated hiding procedure. It is still impossible to retrieve a large number of different secret images from a single host image. Moreover, it is highly desirable that optical implementation complexity can be reduced.

In this paper, a new optical hiding method based on single-input multiple-output (SIMO) and binary amplitude-only holograms (AOHs) via the modified Gerchberg-Saxton algorithm (MGSA) is proposed. The SIMO means that one and only one host image is transmitted, and multiple outputs (i.e., different secret images) can be retrieved from the single host image by using security keys or parameters. In the proposed method, the host image is a binary AOH which is directly generated by using MGSA. In contrast to traditional optical multiple-image hiding methods, the proposed method provides an approach for generating the host image without a superposition of all secret images. Note that the proposed method is different from image sharing and watermarking concepts. When size of the host image is large enough, a large number of different secret images can be retrieved from the host image as verified by our simulations and optical experiments. Moreover, eavesdropping analyses, noise contamination and occlusion contamination have also been numerically and experimentally conducted to demonstrate feasibility and robustness of the proposed method. It is demonstrated by the simulations and optical experiments that the proposed method using the SIMO and binary AOHs via MGSA can greatly enhance the hiding capacity with the reduced optical implementation complexity.

2. Optical hiding based on SIMO and binary AOHs via MGSA

2.1. MGSA

It was shown in conventional Gerchberg-Saxton algorithm [6,18] that the approximate phase distribution of a target image can be iteratively retrieved through a randomly initialized phase distribution and a predefined propagation function, e.g., Fourier transform and Fresnel transform. The Gerchberg-Saxton algorithm has also been developed to retrieve the propagation function. However, there are few studies to apply or modify the Gerchberg-Saxton algorithm to retrieve amplitude information. Amplitude information is usually omitted in conventional Gerchberg-Saxton algorithms, and it is meaningful to explore the field of amplitude holography [19]. In the Gerchberg-Saxton algorithm [6,18], wave propagation from the hologram plane to the Fourier plane can be described by

$$E(x,y) = \frac{exp(jkf)}{j\lambda f} exp\left[\frac{jk}{2f}(x^2+y^2)\right] \times FT\{exp[j\varphi(x_h,y_h)]\}, \tag{1}$$

Optics EXPRESS

where (x_h, y_h) and (x, y) denote coordinates respectively in the hologram plane and the Fourier plane, $\varphi(x_h, y_h)$ denotes phase distribution of a hologram, FT denotes Fourier transform, k denotes wavenumber, λ denotes the wavelength, $j = \sqrt{-1}$, and f denotes focal length. To remove imaginary part for generating amplitude-only hologram, conjugate of the hologram can be used. Then, wave propagation from the hologram plane to the Fourier plane can be described by

$$FT\{\ exp[j\varphi(x_h, y_h)] + exp[-j\varphi(x_h, y_h)]\}\ = FT\{\ 2\cos[\varphi(x_h, y_h)]\}\ , \tag{2}$$

where the image obtained at the Fourier plane contains the retrieved (real) image and a twin image.

Figure 1(a) shows a flow chart of the proposed MGSA for generating AOHs. It starts with an inverse Fourier transform (IFT) of a target image T with a randomly initialized phase φ_n to generate an intermediate phase φ'_n. Subsequently, phase pattern φ'_n is constrained by a cosine function to generate an AOH $\cos(\varphi'_n)$, and then the generated AOH $\cos(\varphi'_n)$ is Fourier transformed to obtain an updated phase pattern φ_{n+1}. Finally, the target image T with the updated phase pattern φ_{n+1} is further inverse Fourier transformed in a new iteration. Once the preset number of iterations is completed, the final AOH is used as the approximated AOH of the target image T. In the case that amplitude retrieval would be too challenging to optically implement, binarization operation is further proposed in the iterative process to reduce the complexity as shown in Fig. 1(b). The generated AOH $\cos(\varphi'_n)$ is binarized by using a simple method as follows:

$$\cos(\varphi'_{nm}) = \begin{cases} 1 & if\ \ \cos(\varphi'_{nm}) \geq \overline{\sum_m \cos(\varphi'_{nm})} \\ 0 & if\ \ \cos(\varphi'_{nm}) < \overline{\sum_m \cos(\varphi'_{nm})} \end{cases}, \tag{3}$$

where m denotes each pixel position in the generated AOH $\cos(\varphi'_n)$, $\sum$ denotes summation of all the pixel values, and $\overline{\sum_m \cos(\varphi'_{nm})}$ denotes mean value of all the pixel values. The binarized hologram φ''_n is further Fourier transformed in the iterative process to update the phase pattern. After the preset number of iterations is completed, an approximated binary AOH of the target image T is generated.

Figures 2(a)–2(i) show typical examples for the binary AOHs generated by using the proposed MGSA and the corresponding retrieved images. Figures 2(a)–2(c) show three different target images, i.e., a simple binary image, a complex binary image and a grayscale image. The corresponding binary AOHs of the target images are generated by using the proposed MGSA with 30 iterations, as shown in Figs. 2(d)–2(f). The correspondingly recovered target images by using Fourier transform are shown in Figs. 2(g)–2(i). Peak signal-to-noise ratio (PSNR) and correlation coefficient (CC) are used to evaluate quality of the retrieved images. Only area of interest in the retrieved images (i.e., the top left corner) is used to calculate PSNR and CC values. PSNR values of the retrieved images (256×256 pixels) respectively corresponding to Figs. 2(g)–2(i) are 15.21 dB, 13.09 dB and 15.57 dB. CC values of the retrieved images in Figs. 2(g)–2(i) are 0.88, 0.95 and 0.88, respectively. In view of the PSNR and CC values, quality of the retrieved images is sufficiently high for information visualization in the optical hiding field.

2.2. Redundancy of binary AOHs

Hologram has shown excellent performance in the conditions of diffuse illumination, scattering and reflections without severe loss of effective information [20–22]. It can be attributed to an extraordinary property of holograms, called redundancy. Holograms have been theoretically and experimentally verified to have a great potential for noise resistance [20–22]. Here, redundancy of binary AOHs generated by using the proposed MGSA is also investigated as shown in Figs. 3(a)–3(i). Binary AOHs contain only 0 and 1 respectively representing black blocks and white blocks in Fig. 3(b). When some white blocks are changed to be black blocks (i.e., changing

Optics EXPRESS

some pixel values in the generated binary AOH from 1 to 0), a degraded binary AOH is further generated as shown in Fig. 3(a). Similarly, an upgraded binary AOH in Fig. 3(c) can be generated by changing some black blocks to be white blocks (i.e., from 0 to 1). According to redundancy characteristic of the holograms, effective information of the target image can still be retrieved from the degraded binary AOH and the upgraded binary AOH at the expense of recovery quality. A typical example of binary AOH generated by using the proposed MGSA is shown in Fig. 3(e) with 512×512 pixels, containing 50% of white blocks (i.e., pixel value of 1) and 50% of black blocks (i.e., pixel value of 0). Its degraded binary AOH in Fig. 3(d) is obtained by randomly selecting 20% of white blocks in Fig. 3(e) to be changed to black blocks. Similarly, its upgraded binary AOH in Fig. 3(f) is obtained by changing 20% of black blocks in Fig. 3(e) to be white blocks. Although the binary AOHs in Figs. 3(d)–3(f) contain different ratios of 0 and 1, effective information of the target image can still be retrieved, as shown in Figs. 3(g)–3(i). PSNR values of Figs. 3(g)–3(i) are 14.18 dB, 18.56 dB and 14.31 dB, respectively. CC values of the retrieved images in Figs. 3(g)–3(i) are 0.57, 0.91 and 0.57, respectively. Compared to quality of the images retrieved by using original binary AOH, that of the images retrieved by using the degraded and

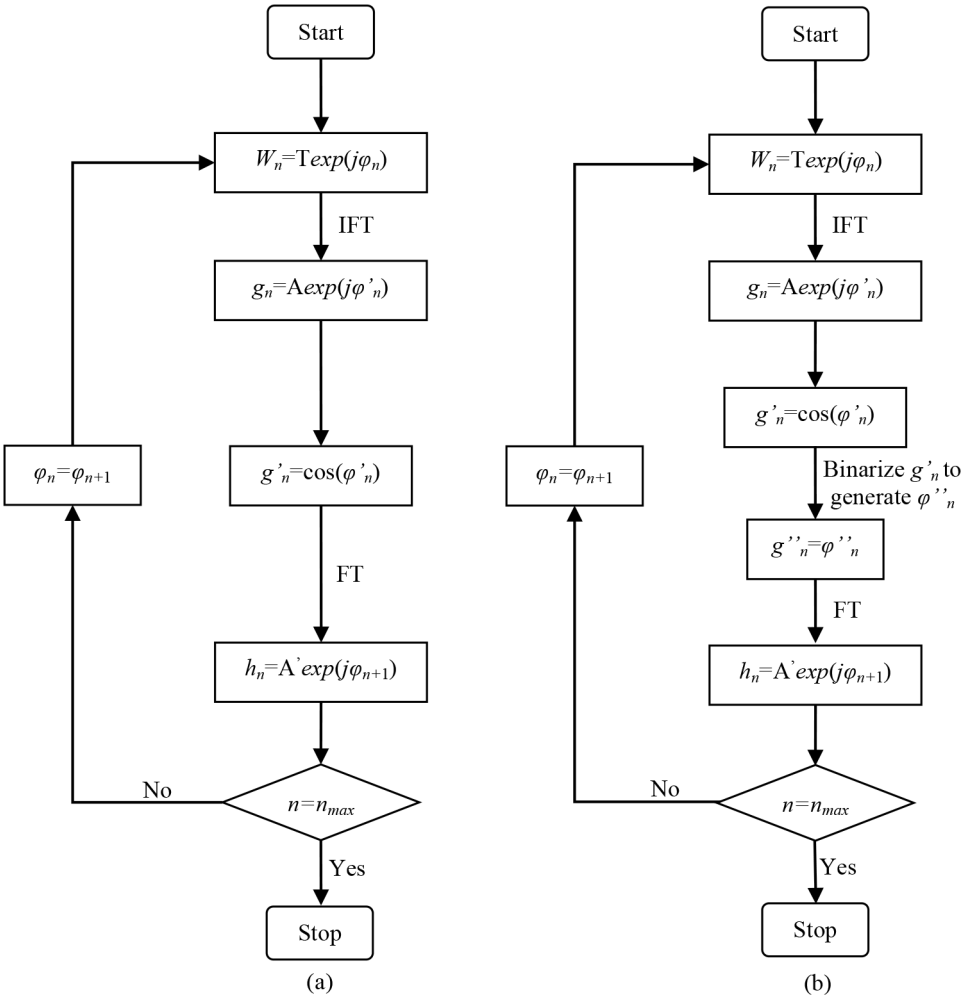


Fig. 1. Flow charts of the proposed MGSA: (a) Flow chart of the proposed MGSA for generating AOHs, and (b) flow chart of the proposed MGSA for generating binary AOHs.

Optics EXPRESS

upgraded binary AOHs decreases slightly and effective information is still visually rendered. Therefore, redundancy provides high robustness for image recovery by using the degraded and upgraded binary AOHs in the proposed method.

To further illustrate effect of redundancy, PSNR and structural similarity index measure (SSIM) are used to evaluate reconstruction quality by using different degraded and upgraded binary AOHs, as shown in Figs. 4(a) and 4(b). The original binary AOH is generated by the proposed MGSA, which contains 50% of white blocks and 50% of black blocks. The reconstructed image is shown in Fig. 4(a1) with PSNR of 12.16 dB and SSIM value of 0.32. It can be seen in Fig. 4(a1) that quality of the recovered image by using original binary AOH is the highest, i.e., the peaks in the curves of PSNR and SSIM versus the percentage. When the degraded AOHs are used, the PSNR values decline with the increased number of black blocks. Figures 4(a2)–4(a6) show the recovered images, when 49%, 40%, 28%, 17% and 8% white blocks are respectively used. The PSNR values of Figs. 4(a2)–4(a6) are 11.83 dB, 9.57 dB, 8.64 dB, 7.90 dB and 7.58 dB, respectively. With the increase of white blocks, upgraded binary AOHs are generated, and PSNR values decrease steadily from the peak by nearly 5.0 dB. When the percentage of white blocks is respectively set as 51%, 60%, 72%, 83% and 92%, PSNR values decline to be 10.91 dB, 9.42 dB, 8.40 dB, 8.32 dB and 7.62 dB in Figs. 4(a7)–4(a11), respectively. Once the percentage of black blocks in the degraded binary AOH or that of white blocks in the upgraded binary AOH approaches a critical value (i.e., 8% and 92%, respectively), effective information of the target image cannot be visually recognized and is contaminated by white stationary noise. In addition, different percentages of white blocks on SSIM values are also studied, as shown in Fig. 4(b). It is

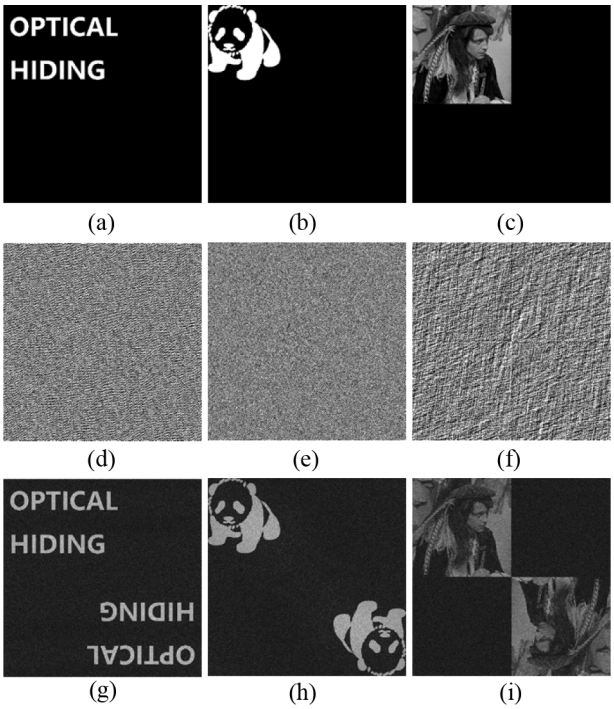


Fig. 2. Typical examples for the binary AOHs obtained by using the proposed MGSA and the corresponding retrieved images: (a)-(c) Target images, (d)-(f) the generated binary AOHs respectively corresponding to (a)-(c), and (g)-(i) the retrieved target images by using the generated binary AOHs respectively in (d)-(f).

Optics EXPRESS

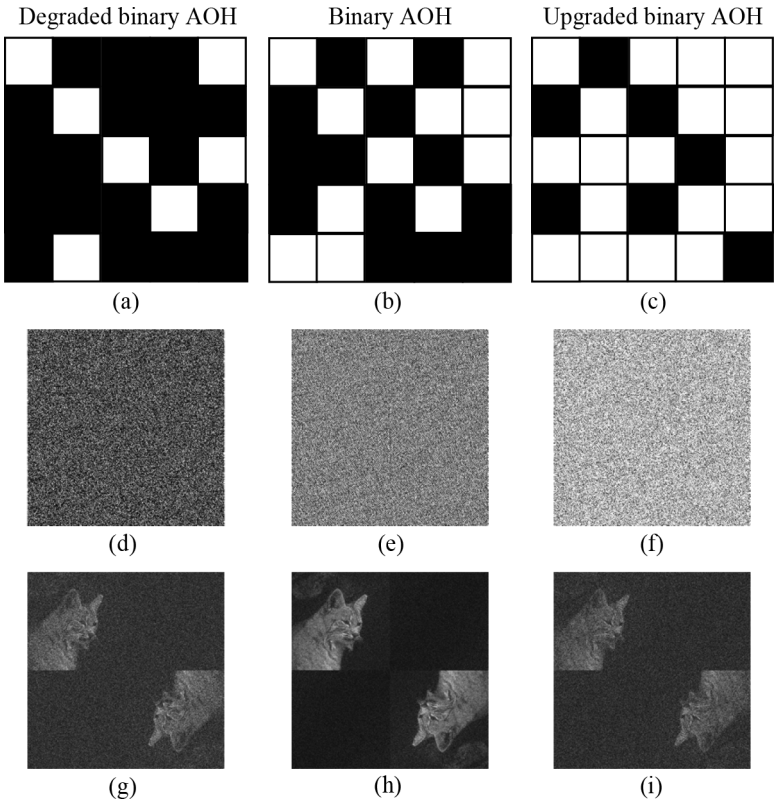


Fig. 3. Redundancy of binary AOHs: (a) schematic of a degraded binary AOH, (b) schematic of original binary AOH, (c) schematic of an upgraded binary AOH, a typical example of (d) the degraded binary AOH, (e) original binary AOH and (f) the upgraded binary AOH, and (g)-(i) the retrieved target images by using the binary AOHs respectively in (d)-(f).

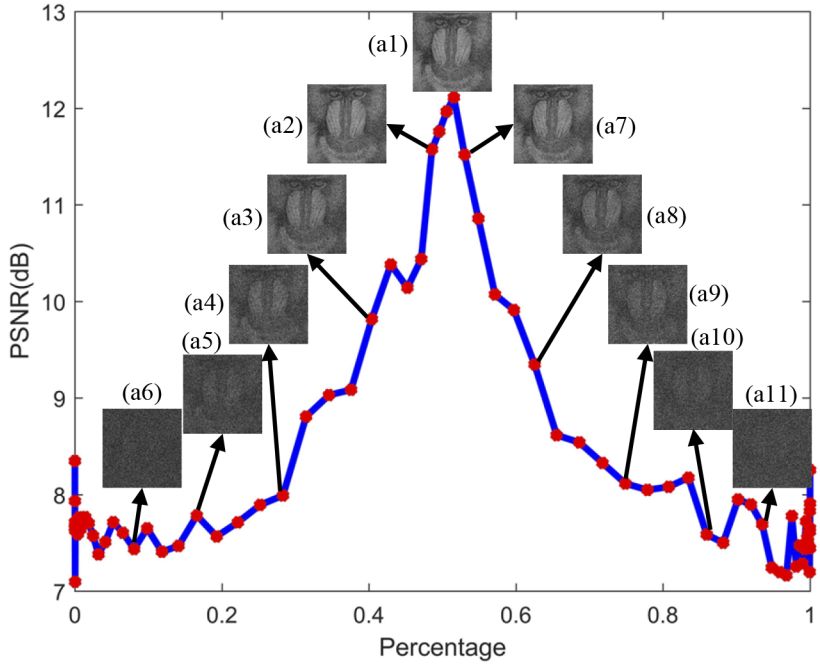
also demonstrated that redundancy of the binary AOHs generated by using the proposed method achieves high robustness.

In this study, AND operator and OR operator are proposed and applied to generate the degraded binary AOHs and the upgraded binary AOHs respectively as shown in Figs. 5(a) and 5(b). In the logistics, AND and OR operators are used to determine a relation between the objects. For AND operator, the expression will be true only if expressions of two objects are true. For OR operator, the expression will be true if one of the expressions is true. AND operator denotes multiplication of expressions, and OR operator denotes summation of expressions. The degraded binary AOHs can be generated by using the AND operator. As shown in Fig. 5(a), an AND operator is applied between each binary AOH and a random binary pattern to generate the degraded binary AOHs, and then the reconstructions are correspondingly conducted by using these degraded binary AOHs with Fourier transform. Figure 5(b) shows that the upgraded binary AOHs can be generated by applying an OR operator between each binary AOH and a random binary pattern, and the reconstructions can be further conducted by using the upgraded binary AOHs with Fourier transform.

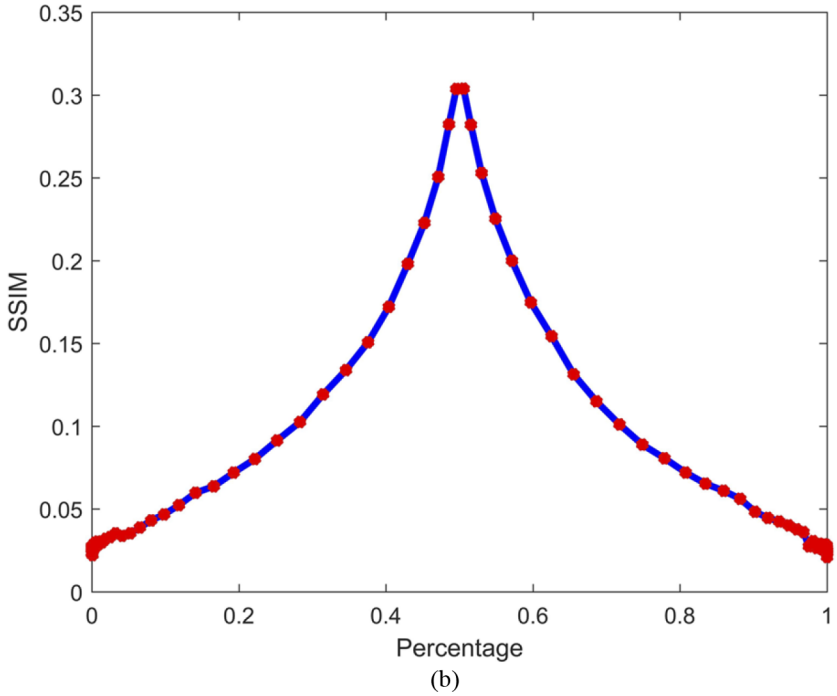
2.3. Optical hiding using SIMO and binary AOHs via MGSA

We have verified the redundancy of binary AOHs generated by using the proposed method, and a new optical hiding strategy based on SIMO and binary AOHs via MGSA is further proposed as

Optics EXPRESS



(a)



(b)

Fig. 4. PSNR and SSIM changed with different percentages of white blocks in binary AOHs. (a) PSNR values changed with different percentages of white blocks in original binary AOH, and (b) SSIM values changed with different percentages of white blocks in original binary AOH. The insets (a2)-(a6) show the recovered images respectively corresponding to 49%, 40%, 28%, 17% and 8% white blocks. The insets (a7)-(a11) show the recovered images respectively corresponding to 51%, 60%, 72%, 83% and 92% white blocks.

Optics EXPRESS

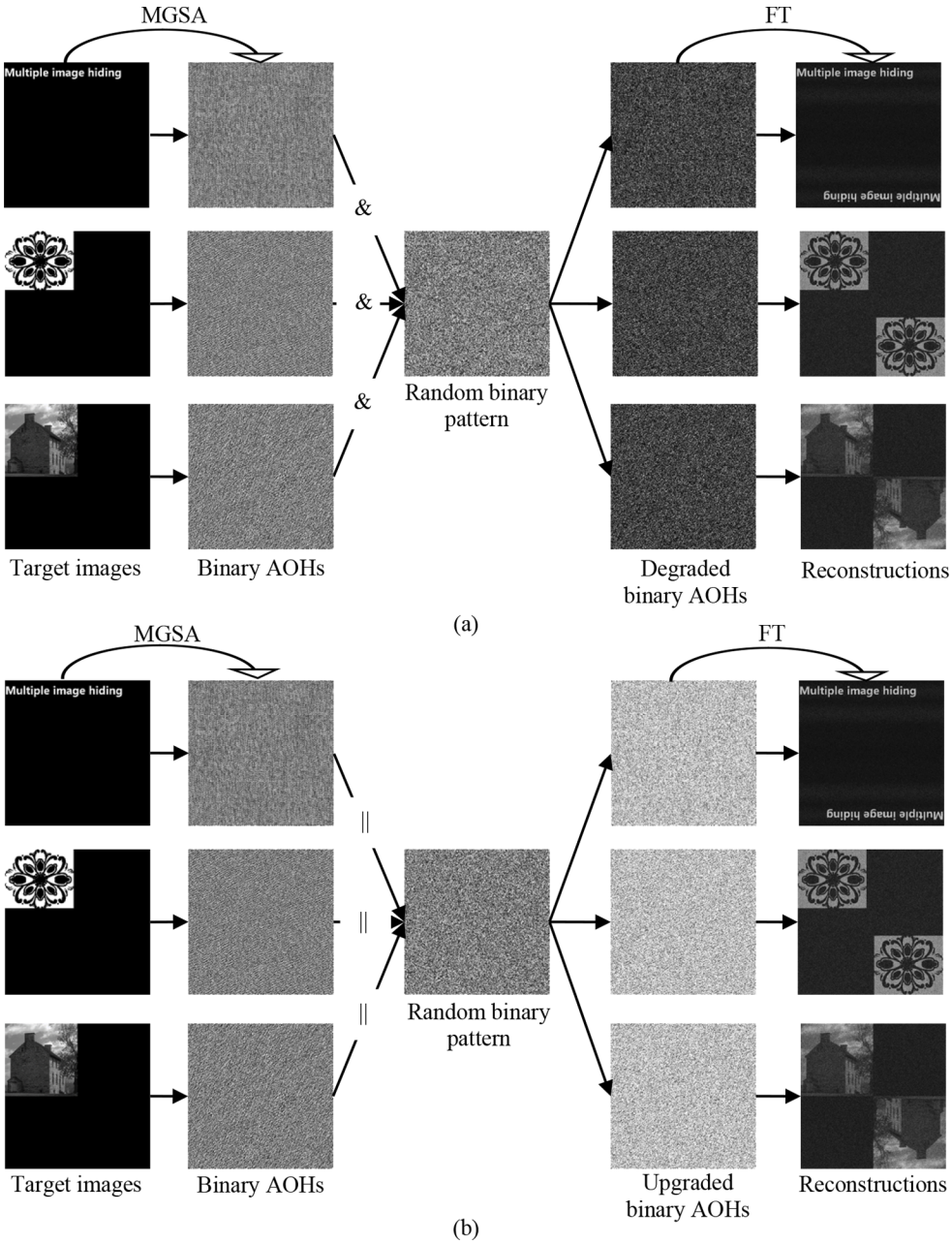


Fig. 5. AND (&) and OR (| |) operators enabled generation of the degraded and upgraded binary AOHs: (a) schematic of AND operator (&) for generating the degraded binary AOHs, and (b) schematic of OR operator (| |) for generating the upgraded binary AOHs.

Optics EXPRESS

shown in Figs. 6(a)–6(c). The proposed optical hiding scheme is described as follows: Figure 6(a) shows the generation of a single host image, and Fig. 6(b) shows a flow chart for security key generation. Figure 6(c) shows the image retrieval process in the proposed method. Without usage of any multiplexing technique, one single host image is directly generated via the proposed MGSA as shown in Fig. 6(a). Two randomly selected images, called arbitrary image (A) and base image (B), are sent to the developed MGSA, and the corresponding binary AOHs are generated as HoloA and HoloB, respectively. It is worth noting that images (A) and (B) are randomly selected images. Subsequently, HoloB is further processed by adding noise, which means that some pixel values in the HoloB are converted from 0 to 1 leading to noisy HoloB. Then, an OR operation is implemented between HoloA and the noisy HoloB to generate a host image. In essence, the host image (C) can be considered as the upgraded binary AOH of HoloA or HoloB. As discussed above, it is feasible to retrieve effective information from the upgraded binary AOHs. To avoid information disclosure of images (A) and (B), additive noise is applied onto HoloB. Then, original information of images (A) and (B) cannot be extracted from the host image. In other words, direct retrieval from the host image cannot provide any effective information related to images (A) and (B). In fact, noise can also be added to HoloA, or to both HoloA and HoloB. Here, it is an exemplification to add noise to HoloB for the demonstration of the proposed method. In this study, generation of the single host image is independent from the secret images, and a large number of different secret images can be retrieved by using the single host image with the corresponding security keys. In the proposed method, security key is generated for each secret image, as shown in Fig. 6(b). The security key generation procedure is as follows: An arbitrary secret image (P_n) is sent to the proposed MGSA to retrieve its corresponding binary AOH HoloP_n. Then, an AND operation is implemented between HoloP_n and the single host image (C) to obtain a degraded binary AOH (HoloP'_n). As discussed in Section 2.2, the degraded

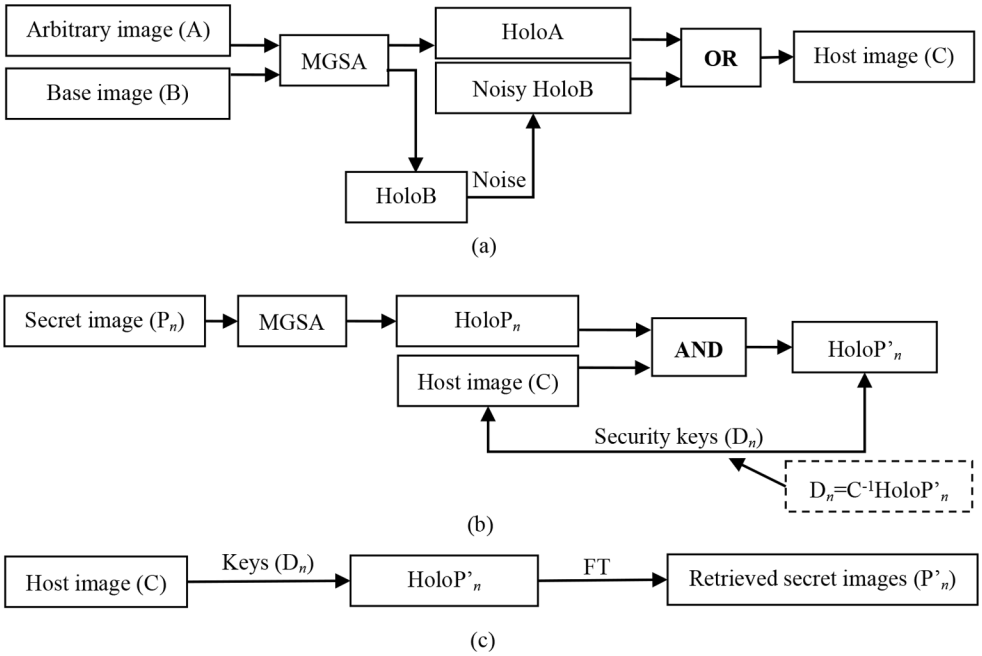


Fig. 6. The proposed scheme based on SIMO and binary AOHs via MGSA: (a) a flow chart for the generation of one single host image (C), (b) a flow chart for the generation of security keys D_n (n=1,2,3,. . .), and (c) a flow chart for optical image retrieval process in the proposed method.

Optics EXPRESS

binary AOH (HoloP'$_n$) can also be used to retrieve effective information of the secret image (P_n). When accurate information of HoloP'$_n$ is obtained, information of P_n can be effectively recovered. Therefore, security key (D_n) for the secret image (P_n) retrieval can be generated by

$$D_n = C^{-1}\text{HoloP}'_n, \tag{4}$$

where C^{-1} denotes the inverse of C, and n denotes an arbitrary number of different secret images. Since the single host image is analytically generated, reversibility of the single host image can be easily realized. When an authorized person possesses correct key D_n, HoloP'$_n$ can be obtained by

$$\text{HoloP}'_n = CD_n. \tag{5}$$

Figure 6(c) shows that a large number of different secret images can be effectively retrieved by using only one single host image, i.e., Eq. (5) with security keys. In the proposed method, for different secret images, different security keys can be generated by using Eq. (4). In other words, many different secret images can be retrieved from the same host image (C) by using their corresponding security keys. Therefore, it is proposed that a large number of different secret images can be extracted from one single host image, when correct security keys are respectively used in the image retrieval process, as shown in Fig. 7. When correct keys (i.e., D_1, D_2, . . . , D_n) are used in Eq. (5), their corresponding binary AOHs (i.e., HoloP'$_1$, HoloP'$_2$, . . . , HoloP'$_n$) can be retrieved. Then, the secret images (i.e., P_1, P_2, . . . , P_n) can be effectively extracted from the retrieved binary AOHs by using Fourier transform. As can be seen in Fig. 7, different secret images can be retrieved from the generated single host image by using correct security keys. This proposed scheme is called as SIMO in this study, which means that there is one and only one input (i.e., the single host image) and many different outputs can be obtained by using the

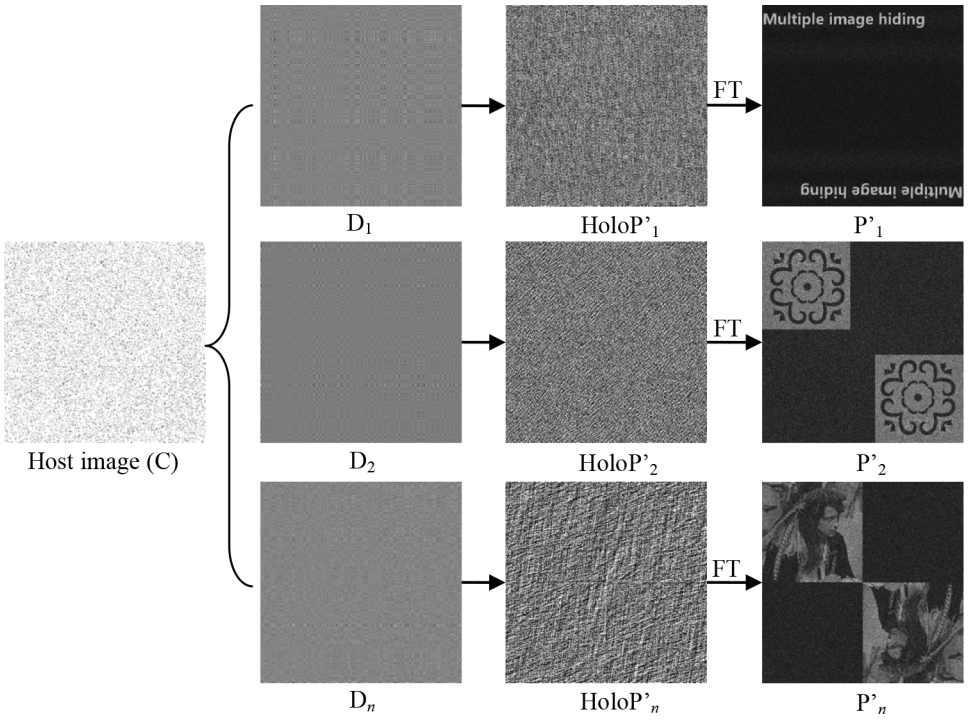


Fig. 7. A schematic for optical image retrieval process (n=1,2,3,. . .) in the proposed method.

Optics EXPRESS

corresponding security keys. Instead of the multiplexing techniques in conventional methods, it is feasible in the proposed method to implement optical multiple-image hiding. The proposed method is advantageous over conventional methods in practical applications, since it is feasible to hide a large number of different secret images and optical implementation complexity is reduced. One point to be highlighted is that security keys change with the secret images.

3. Simulations and optical experiments

3.1. Simulation results and discussion

Simulation work is first conducted to verify feasibility and effectiveness of the developed optical hiding scheme based on the proposed SIMO and binary AOHs via MGSA. The arbitrary image (A) and base image (B) used to generate a single host image (C) are shown in Figs. 8(a) and 8(b), respectively. As discussed above, images (A) and (B) are randomly selected. Here, it is an exemplification that image (A) is a binary image with 512×512 pixels, and image (B) is a grayscale image with 512×512 pixels. Using the steps given in Fig. 6(a) with additional noise of 90%, a host image is generated as shown in Fig. 8(c).

(a) (b) (c)

Fig. 8. Arbitrary image (A) and base image (B) used to generate a single host image (C): (a) an arbitrary image (A), (b) a base image (B), and (c) a single host image generated by using the proposed method.

A large number of different secret images can be concealed by using the proposed method, and here 4 secret images in Figs. 9(a)–9(d) are used as a typical example to illustrate the proposed method. Size of the secret images is 512×512 pixels. Security keys for each secret image are generated by using Eq. (4), i.e., those in Figs. 9(e)–9(h) respectively for the secret images in Figs. 9(a)–9(d). Then, during the process of optical image retrieval, the corresponding binary AOHs can be first retrieved from the single host image using Eq. (5) with correct security keys, i.e., those in Figs. 10(a)–10(d) for the secret images respectively in Figs. 9(a)–9(d). Finally, Fourier transform is implemented to extract the secret images from the retrieved binary AOHs, and the correspondingly retrieved images are shown in Figs. 10(e)–10(h). PSNRs for the retrieved secret images in Figs. 10(e)–10(h) are 13.69 dB, 17.84 dB, 15.18 dB and 19.86 dB, respectively. The CC values for the retrieved secret images in Figs. 10(e)–10(h) are 0.71, 0.86, 0.83 and 0.86, respectively. When wrong security keys D_n are used during the process of optical image retrieval, the retrieved binary AOHs are Fourier transformed and then information of the secret images cannot be visually rendered as shown in Figs. 11(a)–11(d). Feasibility and effectiveness of the proposed method are fully verified. A large number of different secret images (including binary images and grayscale images) can be retrieved from the single host image by using the proposed SIMO scheme. Compared to traditional optical multiple-image hiding methods, the proposed method using SIMO and binary AOHs via MGSA can recover a large number of different secret images from the single host image (C). In addition, the retrieval quality is not affected by the number of secret images to be concealed in the proposed method.

Optics EXPRESS

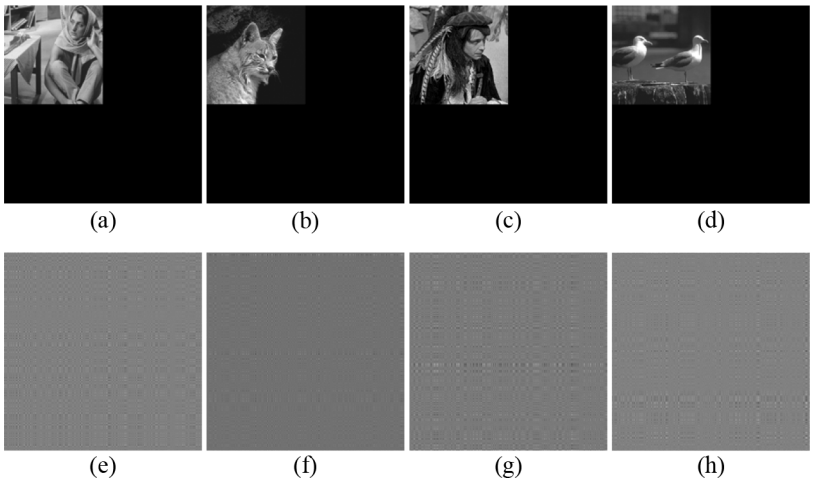


Fig. 9. The secret images and the corresponding security keys: (a)-(d) Secret images, and (e)-(h) the generated security keys respectively corresponding to (a)-(d).

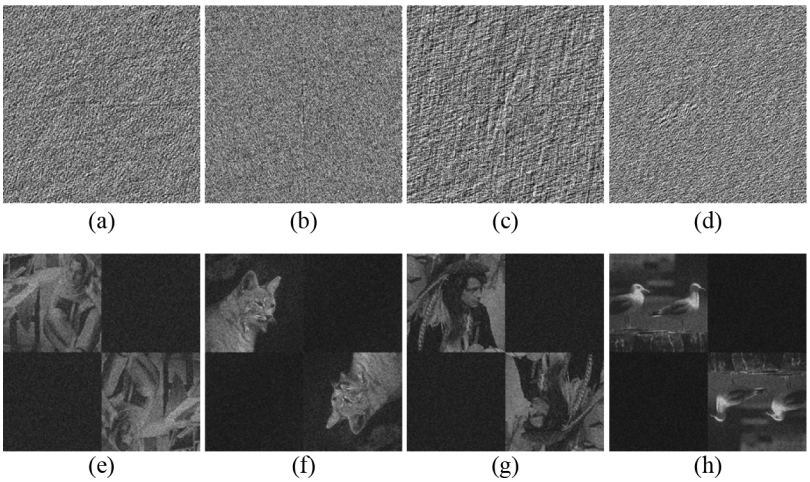


Fig. 10. Optical image retrieval results using the proposed scheme: (a)-(d) The retrieved binary AOHs for the secret images respectively in Figs. 9(a)–9(d), and (e)-(h) the retrieved secret images obtained by using (a)-(d) with correct security keys and Fourier transform.

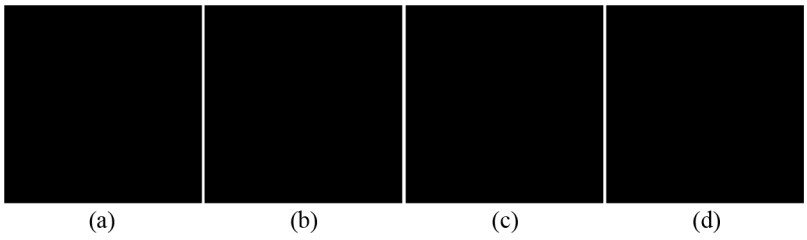


Fig. 11. Optical image retrieval results obtained by using the proposed method with wrong security keys D_n respectively for each of the secret images in Figs. 9(a)–9(d).

Optics EXPRESS

3.2. Security and robustness analyses

Eavesdropping analysis is further conducted to evaluate the proposed method. Figure 12 shows the effect of security keys used in the optical image retrieval process, when a grayscale image is used as the secret image. In Fig. 12, PSNR value of the retrieved images decreases from the highest point (19.86 dB), and then remains steady at around 10 dB. Figures 12(a1)–12(a8) show several retrieved images using different eavesdropping percentages (i.e., 100%, 99.996%, 99.991%, 99.986%, 99.981%, 99.976%, 99.971% and 99.966%), and PSNR values of the retrieved images are 19.86 dB, 14.40 dB, 11.14 dB, 10.83 dB, 10.47 dB, 10.29 dB, 10.23 dB and 10.32 dB, respectively. As can be seen in Fig. 12, when the eavesdropping percentage of security keys is lower than 99.966%, retrieved images cannot visually render any effective information of the secret images. Hence, the eavesdropping analyses demonstrate that high security can be fully guaranteed in the proposed method.

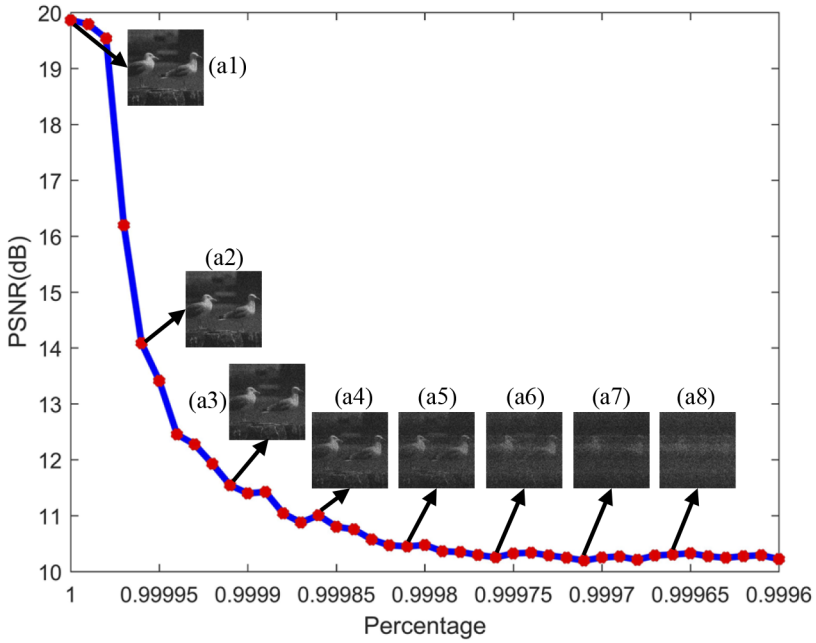


Fig. 12. Eavesdropping analysis of security keys: PSNR values versus eavesdropping percentages when a grayscale image is used as the secret image in the proposed method.

After the proposed method is vetted through eavesdropping analyses, robustness of the proposed optical hiding scheme against noise is also investigated. Figure 13 shows the effect of noise contamination on security keys D_n, when a grayscale image is respectively used as the secret image. In this study, Gaussian noise with mean of 0 and standard deviation of 1 is used and added to security keys D_n. Figure 13 shows the performance of the proposed method with noise contamination on security keys, when a grayscale image is used as secret image. In Fig. 13, there is a sharp decrease of PSNR values for the retrieved images with the increased magnitude of Gaussian noise on security keys. In Figs. 13(a1)–13(a3), PSNR values of the retrieved images are 15.18 dB, 8.48 dB and 7.93 dB, respectively corresponding to the magnitude of Gaussian noise of 0, 0.001 and 0.002. Figure 13(a4) shows a full relationship between PSNR values and the magnitudes of Gaussian noise on security keys D_n. It is demonstrated that security keys in the proposed optical information hiding scheme are robust against noise contamination.

Influence of noise contamination on the single host image (C) is also studied to verify effectiveness and robustness of the proposed method. When a grayscale image is used as secret

Optics EXPRESS

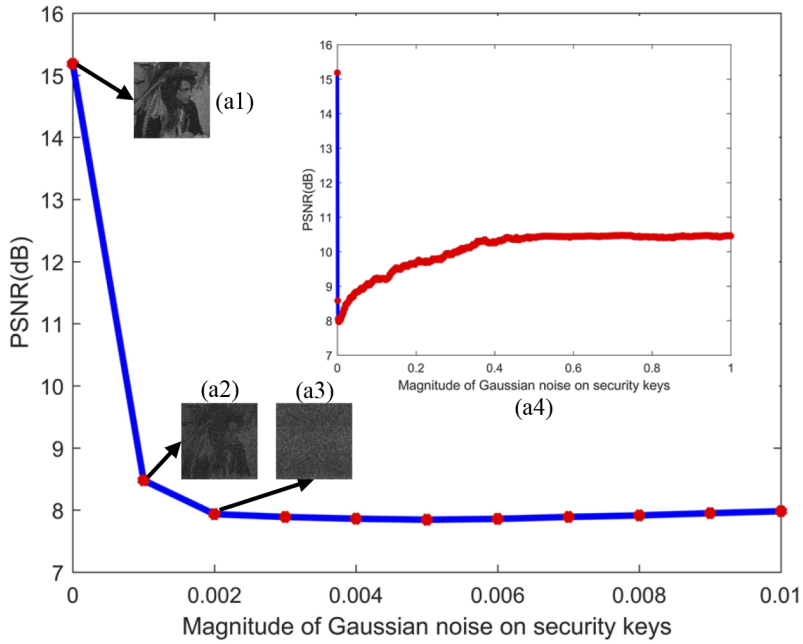


Fig. 13. Relationship between PSNR values and magnitudes of Gaussian noise on security keys D_n: PSNR values versus magnitudes of Gaussian noise on security keys when a grayscale image is used as the secret image.

image as shown in Fig. 14, PSNR values for the retrieved images in Figs. 14(a1)–14(a4) are 17.84 dB, 12.34 dB, 10.79 dB and 10.56 dB, respectively corresponding to the magnitude of Gaussian noise of 0, 0.01, 0.02 and 0.03. When the magnitude of Gaussian noise on the single host image is higher than 0.03, the retrieved images cannot visually render useful information about the secret image. Figure 14(a5) shows the relationship by further increasing the magnitude of Gaussian noise on the single host image (C) to 1, and there is a downward trend of PSNR values with the continuously increased noise magnitudes. It is demonstrated again that the proposed method has high robustness against noise contamination.

Occlusion contamination on the single host image (C) is also studied to demonstrate the performance of the proposed optical hiding scheme. As shown in Fig. 15, the single host image is occluded with the increased percentages, and the occluded region is from the upper left to the lower right. With the increase of occlusion percentage, PSNR values decrease and then remain steady as shown in Fig. 15. When the occlusion percentage increases from 0.000381% to 0.99%, quality of the retrieved images (i.e., the PSNR values) decreases from 17.90 dB to 9.52 dB when a grayscale image is used as the secret image, as respectively shown in Figs. 15(a1) and 15(a2). When the single host image is occluded by 78% as shown in Fig. 15(a3), it can still be feasible to retrieve the secret images and the corresponding PSNR value of the retrieved secret image is 9.14 dB. It is demonstrated that partial loss of the single host image will not affect secret image acquisition during the process of optical image retrieval. This phenomenon can be ascribed to redundancy of the generated binary AOHs. However, when the occlusion percentage reaches 96%, the secret images cannot be recognized from the retrieved image, as shown in Fig. 15(a4) with PSNR value of 9.56 dB.

Based on the above analyses related to eavesdropping, noise contamination and occlusion contamination, it is demonstrated that the proposed optical hiding scheme has high key sensitivity

Optics EXPRESS

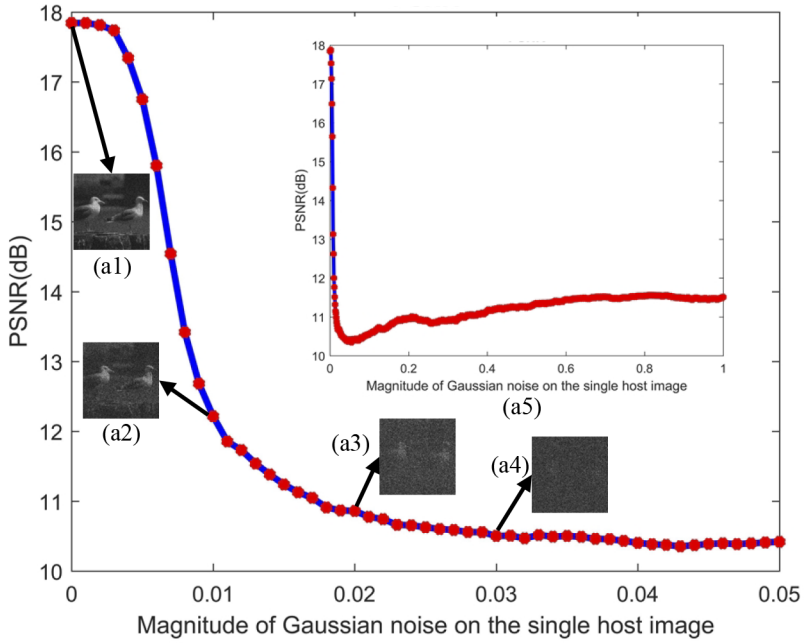


Fig. 14. Relationship between PSNR values and magnitudes of Gaussian noise on the single host image: PSNR values versus magnitudes of Gaussian noise on the single host image when a grayscale image is used as the secret image.

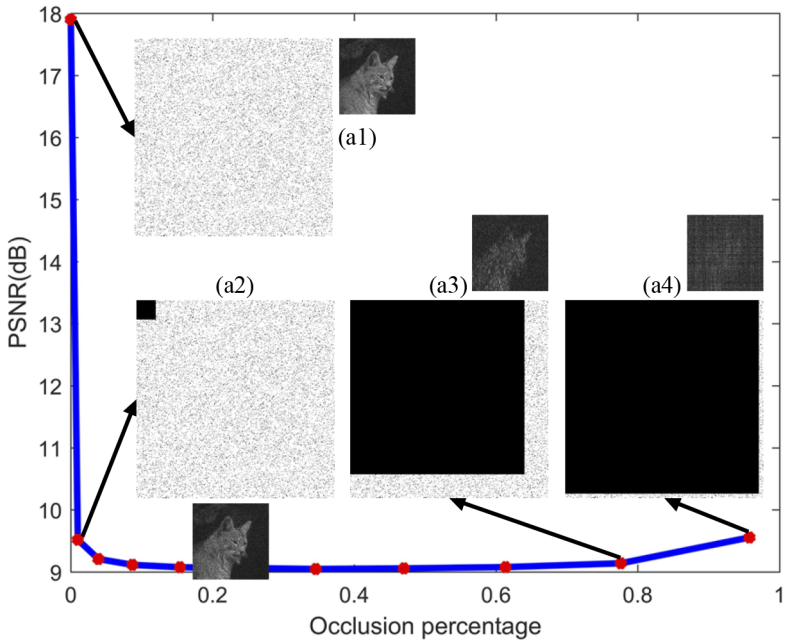


Fig. 15. Occlusion analysis of the single host image: PSNR values versus occlusion percentages of the single host image when a grayscale image is used as the secret image.

Optics EXPRESS

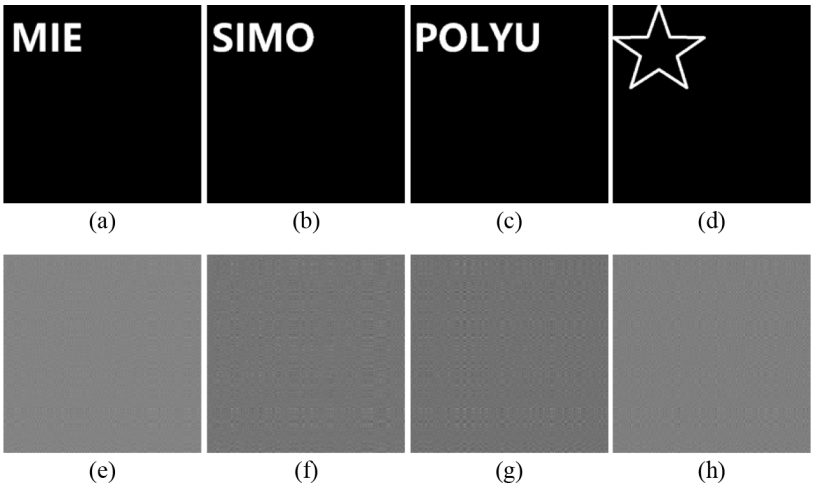
and high security. Moreover, the proposed method shows high robustness, since it is resistant to noise contamination and occlusion contamination.

3.3. Optical experiments and result discussion

To fully demonstrate feasibility and effectiveness of the proposed optical hiding scheme based on SIMO and binary AOHs via MGSA, optical experiments are also conducted for optical retrieval (i.e., de-multiplexing) [18,23,24]. In the optical experiments, images (A) and (B) used to generate a single host image are shown in Figs. 16(a) and 16(b), respectively. Using the steps in Fig. 6(a), a host image is generated as shown in Fig. 16(c) with additional noise of 90%. Due to the limitation of high-resolution optical devices in the lab, four binary images are used to be secret images as a typical example for verifying the proposed method in our optical experiments as shown in Figs. 17(a)–17(d). Security keys D_n for these secret images are correspondingly generated and shown in Figs. 17(e)–17(h). To retrieve different secret images from the single host image (C) in optical experiments, it is necessary to retrieve their corresponding binary AOHs ($HoloP'_n$) by using $HoloP'_n=CD_n$ with correct security keys (D_n), and then Fourier transform can be experimentally conducted to extract or record secret images from the retrieved binary AOHs. By using correct security keys, the corresponding binary AOHs are retrieved from the single host image as shown in Figs. 18(a)–18(d), respectively corresponding to the four different secret images in Figs. 17(a)–17(d).

(a) (b) (c)

Fig. 16. Information hiding process in the proposed optical hiding scheme based on SIMO and binary AOHs via MGSA: (a) An arbitrary image (A) with 512×512 pixels, (b) a base image (B) with 512×512 pixels, and (c) a single host image (C) with 512×512 pixels.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 17. The secret images and the corresponding security keys: (a)-(d) secret images, and (e)-(h) the generated security keys D_n respectively corresponding to (a)-(d).

Optics EXPRESS

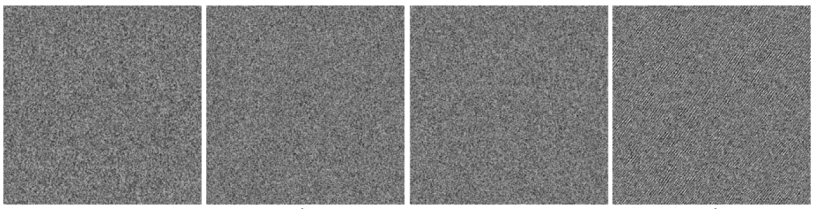


Fig. 18. The retrieved binary AOHs from the single host image using correct security keys.

Optical experiments are conducted to extract the secret images from the retrieved binary AOHs, and a schematic experimental setup is shown in Fig. 19. A He-Ne laser with wavelength of 633 nm (Newport, R-30993) is expanded by an objective lens (Newport, M-40X, 0.65 NA), and then is collimated by a lens. The collimated light is reflected by a mirror to illuminate a spatial light modulator (SLM, Holoeye LC-R720). The retrieved binary AOHs are sequentially embedded into the SLM, and then the modulated wave transmits through a lens (f=10 cm) before being recorded by a CCD camera with 1280×1024 pixels and pixel size of 5.30 μm (Thorlabs, DCC3240M). Finally, the images recorded by CCD, i.e., the retrieved secret images, are shown in Fig. 20. It can be seen in Figs. 20(a)–20(d) that the secret images have been successfully extracted from the retrieved binary AOHs. It is experimentally verified that a large number of different secret images can be retrieved from the single host image by using the proposed SIMO scheme with security keys. Due to misalignment of CCD and difficulties of pixel-to-pixel calibration, shape of original secret images is changed. Hence, visibility rather than PSNR is calculated to evaluate quality of the retrieved secret images, which is defined as [25,26]

$$\text{Visibility} = \frac{<I_s> - <I_b>}{<I_s> + <I_b>}, \tag{6}$$

where I_s and I_b denote intensity respectively in the signal part (indicated by the red block with effective information of the retrieved secret images) and the background part (noisy part without any effective information of the retrieved secret images), and $< I_s >$ and $< I_b >$ respectively denote average intensity of the signal part and the background part. Visibility values for the retrieved secret images in Figs. 20(a)–20(d) are 0.96, 0.94, 0.94 and 0.97, respectively. It is illustrated that information of the secret images is fully recognized and visually rendered, which is sufficient in the optical hiding field.

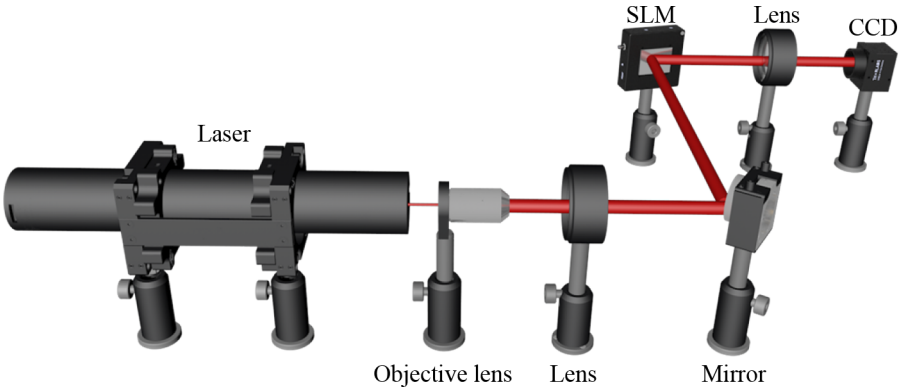


Fig. 19. Schematic experimental setup for the proposed method based on SIMO and binary AOHs via MGSA. SLM: spatial light modulator; CCD: charge-coupled device.

Optics EXPRESS

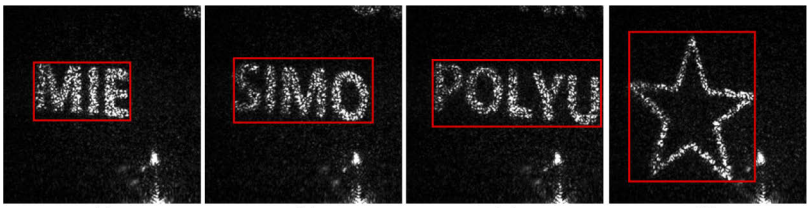


Fig. 20. The four secret images recorded in optical experiments using correct security keys. The signal part is indicated by red block.

When wrong security keys D_n are used for optical image retrieval, the retrieved binary AOHs are shown in Figs. 21(a)–21(d). The retrieved binary AOHs are sequentially embedded into the SLM, and Figs. 21(e)–21(h) show the retrieved images recorded by the CCD which cannot visually render any information of the secret images respectively in Figs. 17(a)–17(d).

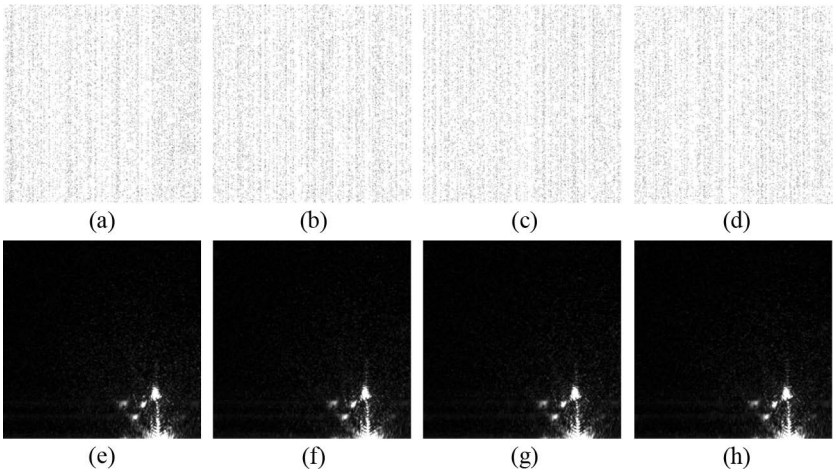


Fig. 21. Optical experimental results using wrong security keys D_n: (a)-(d) The retrieved binary AOHs using wrong security keys D_n, and (e)-(h) the secret images recorded by the CCD respectively corresponding to (a)-(d).

Eavesdropping analysis of security keys D_n is also conducted by using optical experimental results to verify the proposed optical hiding scheme. Figure 22 shows the eavesdropping analysis of security keys D_n for a secret image. The binary AOHs in Figs. 22(a)–22(e) are retrieved by using the different eavesdropping percentages (i.e., 99.999%, 99.959%, 99.919%, 99.879% and 99.839%) of security keys D_n, and the corresponding secret images are extracted by the CCD as shown in Figs. 22(f)–22(j). Visibility values for the retrieved secret images in Figs. 22(f)–22(j) are 0.96, 0.95, 0.91, 0.85 and 0.71, respectively. It can be seen in Figs. 22(f)–22(j) that quality of the retrieved secret images decreases with the decreased eavesdropping percentages of security keys D_n. When the eavesdropping percentage of security keys is lower than 99.839%, the retrieved image cannot visually render any effective information about the secret image, as shown in Fig. 22(j). It is experimentally verified that high security is fully achieved in the proposed method.

Influence of noise contamination on security keys and the single host image is also investigated to verify the proposed method, as shown in Figs. 23 and 24. Figures 23(a)–23(h) show the influence of Gaussian noise (mean of 0 and standard deviation of 1) on security keys D_n. When

Optics EXPRESS

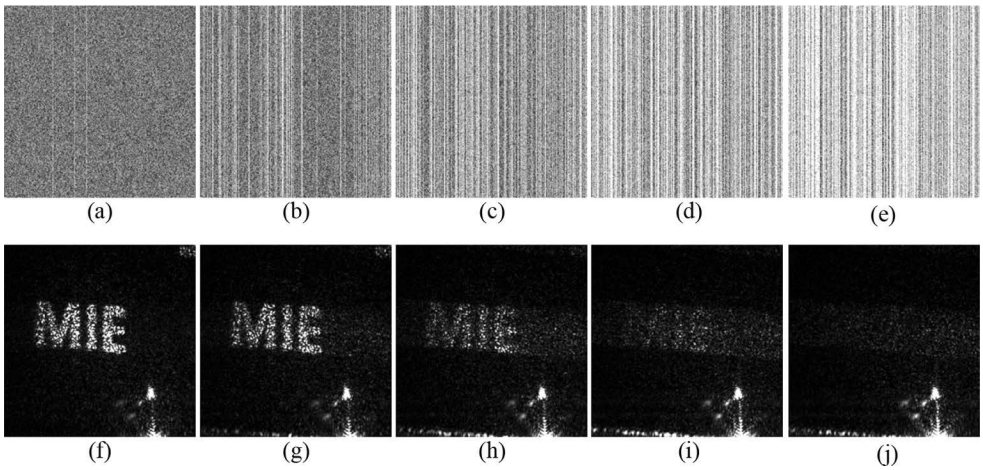


Fig. 22. Eavesdropping analysis of security keys D_n in optical experiments: (a)-(e) The retrieved binary AOHs with eavesdropping percentages of 99.999%, 99.959%, 99.919%, 99.879% and 99.839% of security keys when the "MIE" image is used as the secret image. (f)-(j) The recorded secret images respectively corresponding to (a)-(e).

the magnitude of Gaussian noise added to security keys D_n is 0.001, the retrieved binary AOHs are shown in Figs. 23(a) and 23(c). The corresponding secret images are retrieved as shown in Figs. 23(e) and 23(g), and visibility values for the retrieved secret images in Figs. 23(e) and 23(g) are 0.92 and 0.89, respectively. When the magnitude of Gaussian noise is 0.002, the corresponding binary AOHs are retrieved and shown in Figs. 23(b) and 23(d). The correspondingly retrieved secret images are shown in Figs. 23(f) and 23(h), and visibility values for the retrieved secret images are 0.75 and 0.64, respectively. As can be seen in Figs. 23(a)–23(h), quality of the retrieved secret images decreases with the increase of the magnitude of noise added to security keys D_n.

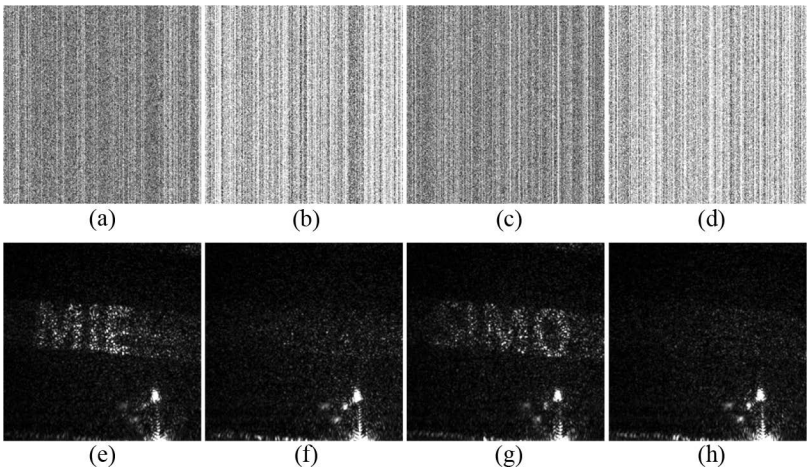


Fig. 23. Noise contamination on security keys D_n: (a) and (c) The retrieved binary AOHs when the magnitude of Gaussian noise is 0.001, and (b) and (d) the retrieved binary AOHs when the magnitude of Gaussian noise is 0.002. (e) and (g) The retrieved secret images respectively corresponding to (a) and (c), and (f) and (h) the retrieved secret images respectively corresponding to (b) and (d).

Optics EXPRESS

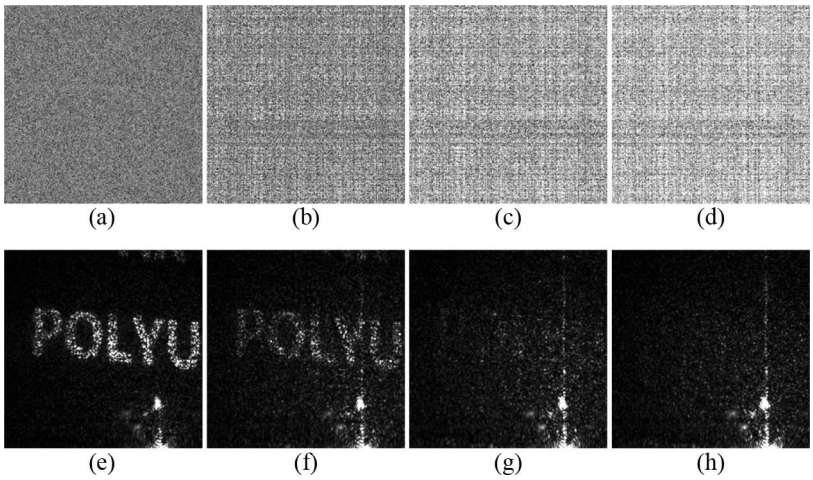


Fig. 24. Noise contamination on the single host image: (a)-(d) The retrieved binary AOHs when magnitude of Gaussian noise is 0.001, 0.01, 0.02 and 0.03, respectively. (e)-(h) The retrieved secret images recorded by the CCD respectively corresponding to (a)-(d).

Figures 24(a)–24(h) show the performance of the proposed method, when there is noise contamination (mean of 0 and standard deviation of 1) on the generated single host image. When the single host image is contaminated by a sequentially increased magnitude of Gaussian noise (i.e., 0.001, 0.01, 0.02 and 0.03), the retrieved binary AOHs for a random secret image are shown in Figs. 24(a)–24(d), respectively. The corresponding secret images are extracted by using the CCD, as shown in Figs. 24(e)–24(h), respectively. Visibility values for the retrieved secret images in Figs. 24(e)–24(h) are 0.94, 0.89, 0.76 and 0.65, respectively. With the increase of magnitude of Gaussian noise added to the single host image, quality of the retrieved secret images decreases. When the magnitude of Gaussian noise increases to be 0.02, the images recorded by the CCD cannot visually render any information about the secret image as shown in Fig. 24(g). Compared to security keys, the single host image can possess the higher robustness against noise contamination during data storage or transmission, which is in accordance with simulation results.

Since the generated host image (C) could also be occluded during data storage or data transmission, occlusion contamination is also experimentally studied as shown in Figs. 25(a)–25(l). Figures 25(a)–25(d) show the occluded host images generated by respectively using different occlusion percentages of 1.00% (50×50 pixels), 46.73% (350×350 pixels), 77.25% (450×450 pixels) and 95.37% (500×500 pixels). The corresponding binary AOHs retrieved from the occluded host images are shown in Figs. 25(e)–25(h) when the "star" image is used as the secret image. Then, the corresponding secret images recorded by CCD are shown in Figs. 25(i)–25(l). Visibility values for the retrieved secret images in Figs. 25(i)–25(l) are 0.97, 0.96, 0.90 and 0.85, respectively. It can be seen in Fig. 25 that quality of the retrieved secret images decreases with the increased occlusion percentages of the single host image. Even when occlusion percentage of the single host image approaches 77.25%, some information related to the secret image can still be recognized as shown in Fig. 25(k). It is experimentally demonstrated that the proposed optical hiding scheme can effectively withstand occlusion contamination. This is also in accordance with simulation results to prove redundancy of the generated binary AOHs in the proposed method.

Effectiveness and robustness of the proposed optical hiding scheme based on SIMO and binary AOHs via MGSA are fully demonstrated by using optical experiments. Without using any multiplexing techniques, a single host image is generated. The proposed method can realize the retrieval of a large number of different secret images using one single host image which can fully

Optics EXPRESS

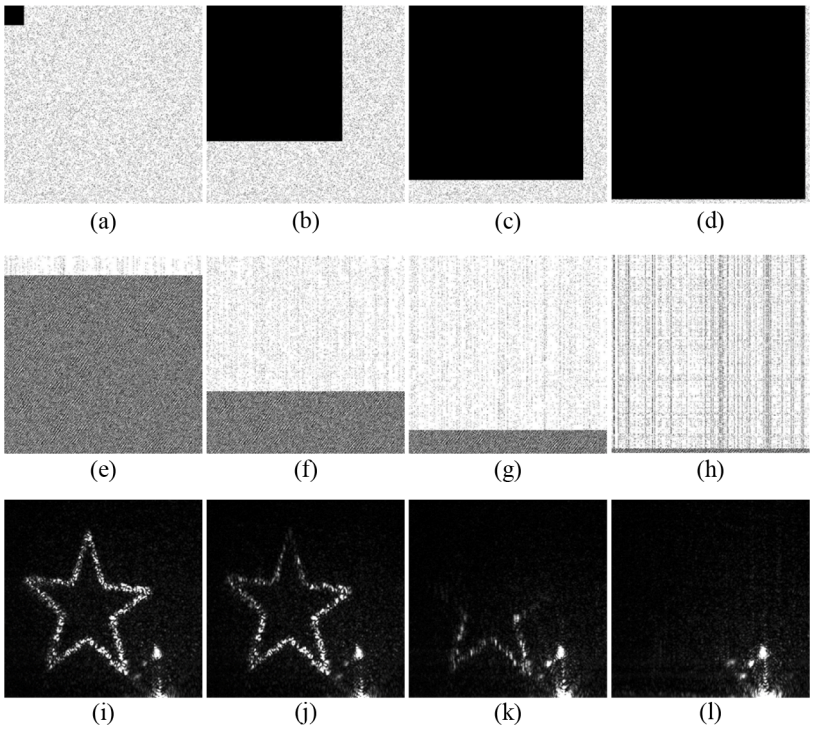


Fig. 25. Occlusion contamination on the single host image (C): (a)-(d) The occluded host image respectively using occlusion percentages of 1.00%, 46.73%, 77.25% and 95.37%. (e)-(h) The retrieved binary AOHs corresponding to (a)-(d) for the "star" secret image. (i)-(l) The retrieved secret images respectively corresponding to (e)-(h).

overcome the challenge existing in conventional methods. In addition, the optical implementation complexity is dramatically reduced.

4. Conclusions

We have proposed a new method for optical hiding based on SIMO and binary AOHs via MGSA. Instead of using multiplexing techniques to superpose all the secret images, a single host image, i.e., one binary AOH, is directly generated by using the proposed MGSA. When size of the host image is sufficiently large, a large number of different secret images (including binary images, grayscale images and color images) can be retrieved by using the single host image with security keys. Simulations and optical experiments have been conducted to fully illustrate validity of the proposed method, and security and robustness of the proposed method have also been fully verified in the simulations and optical experiments.

Funding. National Natural Science Foundation of China (61605165); Hong Kong Research Grants Council (25201416, C5011-19G); Shenzhen Science and Technology Innovation Commission (JCYJ20160531184426473); Hong Kong Polytechnic University (G-R006, 4-R006, 4-ZZLF, 1-W167).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

Optics EXPRESS

1. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**(3), 589–636 (2009).
2. B. Javidi, "Securing information with optical technologies," Phys. Today **50**(3), 27–32 (1997).
3. O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," Proc. IEEE **97**(6), 1128–1148 (2009).
4. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**(2), 120–155 (2014).
5. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
6. X. Wang, W. Chen, and X. Chen, "Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding," Opt. Express **22**(19), 22981–22995 (2014).
7. M. R. Abuturab, "Securing color information using Arnold transform in gyrator transform domain," IEEE Photonics J. **50**(5), 772–779 (2012).
8. Z. Liu, Y. Zhang, W. Liu, F. Meng, Q. Wu, and S. Liu, "Optical color image hiding scheme based on chaotic mapping and Hartley transform," Optics and Lasers in Engineering **51**(8), 967–972 (2013).
9. J. Li, Y. Li, J. Li, Q. Zhang, and J. Li, "Single-pixel compressive optical image hiding based on conditional generative adversarial network," Opt. Express **28**(15), 22992–23002 (2020).
10. M. Otaka, H. Yamamoto, and Y. Hayasaki, "Manually operated low-coherence interferometer for optical information hiding," Opt. Express **14**(20), 9421–9429 (2006).
11. J. Li, J. Li, L. Shen, Y. Pan, and R. Li, "Optical image encryption and hiding based on a modified Mach-Zehnder interferometer," Opt. Express **22**(4), 4849–4860 (2014).
12. L. Wang, S. Zhao, W. Cheng, L. Gong, and H. Chen, "Optical image hiding based on computational ghost imaging," Opt. Commun. **366**, 314–320 (2016).
13. A. Alfalou, C. Brosseau, N. Abdallah, and M. Jrifi, "Simultaneous fusion, compression, and encryption of multiple images," Opt. Express **19**(24), 24023–24029 (2011).
14. Y. Shi, G. Situ, and J. Zhang, "Multiple-image hiding by information prechoosing," Opt. Lett. **33**(6), 542–544 (2008).
15. F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, "All-optical encrypted movie," Opt. Express **19**(6), 5706–5712 (2011).
16. Y. Shi, G. Situ, and J. Zhang, "Multiple-image hiding in the Fresnel domain," Opt. Lett. **32**(13), 1914–1916 (2007).
17. W. Xu, Y. Luo, T. Li, H. Wang, and Y. Shi, "Multiple-image hiding by using single-shot ptychography in transform domain," IEEE Photon. J. **9**(3), 1–10 (2017).
18. H. E. Hwang, H. T. Chang, and W. N. Lie, "Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain," Opt. Lett. **34**(24), 3917–3919 (2009).
19. Z. Xu, L. Huang, X. Li, C. Tang, Q. Wei, and Y. Wang, "Quantitatively correlated amplitude holography based on photon sieves," Adv. Opt. Mater. **8**(2), 1901169 (2020).
20. H. J. Gerritsen, W. J. Hannan, and E. G. Ramberg, "Elimination of speckle noise in holograms with redundancy," Appl. Opt. **7**(11), 2301–2311 (1968).
21. U. Schnars and W. Jueptner, *Digital Holography: Digital Hologram Recording, Numerical Reconstruction, and Related Techniques* (Springer, 2005).
22. T. Kreis, *Handbook of Holographic Interferometry: Optical and Digital Methods* (Wiley-VCH, 2005).
23. W. Liu, Z. Xie, Z. Liu, Y. Zhang, and S. Liu, "Multiple-image encryption based on optical asymmetric key cryptosystem," Opt. Commun. **335**, 205–211 (2015).
24. A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," Appl. Opt. **48**(31), 5933–5947 (2009).
25. S. R. Ghaleh, S. Ahmadi-Kandjani, R. Kheradmand, and B. Olyaeefar, "Improved edge detection in computational ghost imaging by introducing orbital angular momentum," Appl. Opt. **57**(32), 9609–9614 (2018).
26. H. Kellock, T. Setälä, T. Shirai, and A. T. Friberg, "Higher-order ghost imaging with partially polarized classical light," Proc. SPIE **8171**, 81710Q (2011).