photonics

MDPI

Article

Watermarking and Encryption for Holographic Communication

Zehao He *, Kexuan Liu and Liangcai Cao

State Key Laboratory of Precision Measurement Technology and Instruments, Department of Precision Instruments, Tsinghua University, Beijing 100084, China
* Correspondence: hezehao@mail.tsinghua.edu.cn

Abstract: Holographic communication is a three-dimensional (3D) video communication technology based on computer-generated holograms (CGHs) which has the potential to give users a more realistic visual perception. As this is an emerging field, the encrypted encoding and decoding methods in holographic communication have not been widely studied. In this work, a watermarking and encryption method for holographic communication is proposed. A watermark is inserted into the original image using the discrete cosine transform before the calculation of the CGH, while a secret key is employed to produce the encrypted CGH during the holographic calculation. Through the proposed watermarking and encryption method, the signal of holographic communication is difficult to decrypt. Even if the signal is decrypted, the source of the leak is easy to trace due to the existence of the watermark. The watermarking and encryption method can provide a practical solution for the privacy protection and copyright protection of 3D video communication.

Keywords: holographic communication; computer-generated holography; holographic encryption

Citation: He, Z.; Liu, K.; Cao, L. Watermarking and Encryption for Holographic Communication. *Photonics* **2022**, *9*, 675. https://doi.org/10.3390/photonics9100675

Received: 16 August 2022
Accepted: 13 September 2022
Published: 21 September 2022

1. Introduction

The increasing demand for emerging applications including online conferences, remote collaboration, and the metaverse has significantly promoted the development of video communication technology. Compared to conventional two-dimensional (2D) video communication, three-dimensional (3D) video communication provides depth information, which gives users a more immersive experience. Therefore, it has been widely studied in recent years. For example, Holoportation, which is a binocular 3D communication system, demonstrates a high-quality real-time 3D reconstruction of the entire space with an AR helmet [1]; TeleHuman2, which is a cylindrical 3D communication system, conveys a full-body 3D video of interlocutors with a large-size cylindrical screen [2]; Starline, which is a flat 3D communication system, lets two people who are separated by distance have a face-to-face conversation with a light-field display system [3].

Considering the realizability, the monitors of current 3D video communication systems are often designed using binocular 3D displays and light-field 3D displays. In addition to these mentioned display technologies, the holographic 3D display is an option that can be applied in future 3D video communication. It is an approach that realizes 3D reconstruction using the diffractive pattern that records both the amplitude and phase of the 3D target. It presents all the 3D depth cues that human eyes can perceive, providing perfect authenticity and immersion for the users, which is widely considered the ultimate solution for 3D video communication [4].

For the holographic display, the generation of the diffractive pattern can be realized through either the optical configuration or the holographic algorithm. Compared to the optically recorded pattern, the algorithm-generated pattern, which is often called a computer-generated hologram (CGH), has the advantages of better consistency and easier replication. Thus, the CGH-based holographic display shows a better application prospect in the field of 3D video communication.

In a CGH-based holographic communication system, the main concerns can be classified into four categories: the rendering of 3D contents, the calculation of CGHs, the transmission of CGHs, and the construction of the holographic display system. In our previous work, the rendering of 3D contents [5], the calculation of CGHs [6,7], and the construction of the holographic display system [8] have been properly addressed. In this work, the transmission of CGHs is discussed in detail.

To protect privacy and copyright, the signal of holographic communication should keep its encryption during transmission. Holographic encryption has been widely studied since double random phase encoding was proposed [9]. For a CGH-based system, holographic encryption is often realized based on optical diffraction via spatial light modulators (SLMs) [10–16]. However, for the application of holographic communication, these encryption approaches are limited by the computational load and the system complexity. A general and efficient encryption method independent of the holographic display system is significantly necessary for holographic communication. Additionally, if the encrypted signal is decrypted by non-target users, the source of the leak should be easy to trace. In traditional video communication, by inserting a watermark containing some important information including the IP address and account number of a target user into the original image, the source of the leak can be readily traced [17–22]. However, for holographic communication, the encoding and reconstruction of the CGHs bring a lot of noise into the displayed images [23]. Influenced by the introduced noise, the watermark inserted into the original image might be difficult to extract. The watermark insertion and noise elimination should be conducted simultaneously.

In this work, a watermarking and encryption method for holographic communication is proposed. A watermark is inserted into the original image using discrete cosine transform (DCT) before the calculation of the CGH. An iterative angular spectrum method (IASM) is used to eliminate the noise introduced through the encoding and reconstruction of the CGHs. A secret key is employed to produce the encrypted CGH during the holographic calculation. Through this method, the signal is encrypted and watermarked, protecting privacy and copyright in holographic communication.

2. Methods

The signal side and the display side of the holographic communication system are shown in Figure 1a,b, respectively. On the signal side, the original image to be displayed is first watermarked using DCT. Then, the watermark that is used as the tracking tag is hidden in the processed image, which cannot be observed by human eyes. To encode the watermarked image into a CGH, the accuracy of the holographic algorithm should be considered. If the accuracy of the obtained CGH is inadequate, the error introduced during the calculation would appear as speckle noise in the holographic reconstruction. The speckle noise is likely to disturb the inserted watermark, making it difficult to be extracted. Therefore, an accurate holographic calculation method called IASM is employed to obtain the unencrypted CGH from the watermarked image. To enhance the confidentiality of the transmission, the obtained CGH is then encrypted via a secret key, which is essentially a pseudo-random phase. The encrypted CGH can be transferred from the signal side to the display side by the routers.

On the display side, the received CGH is first decrypted using the same secret key. The decrypted CGH is then uploaded onto a phase-only SLM and illuminated with a coherent plane wave. After the optical reconstruction, the displayed image can be observed by the human eye. If a user records and disseminates the image contents without permission, the inserted watermark can be extracted from the recorded image using DCT. According to the information in the watermark, the source of the leak can easily be traced. The detailed processes of watermark insertion and holographic encryption and decryption are described in the following parts.

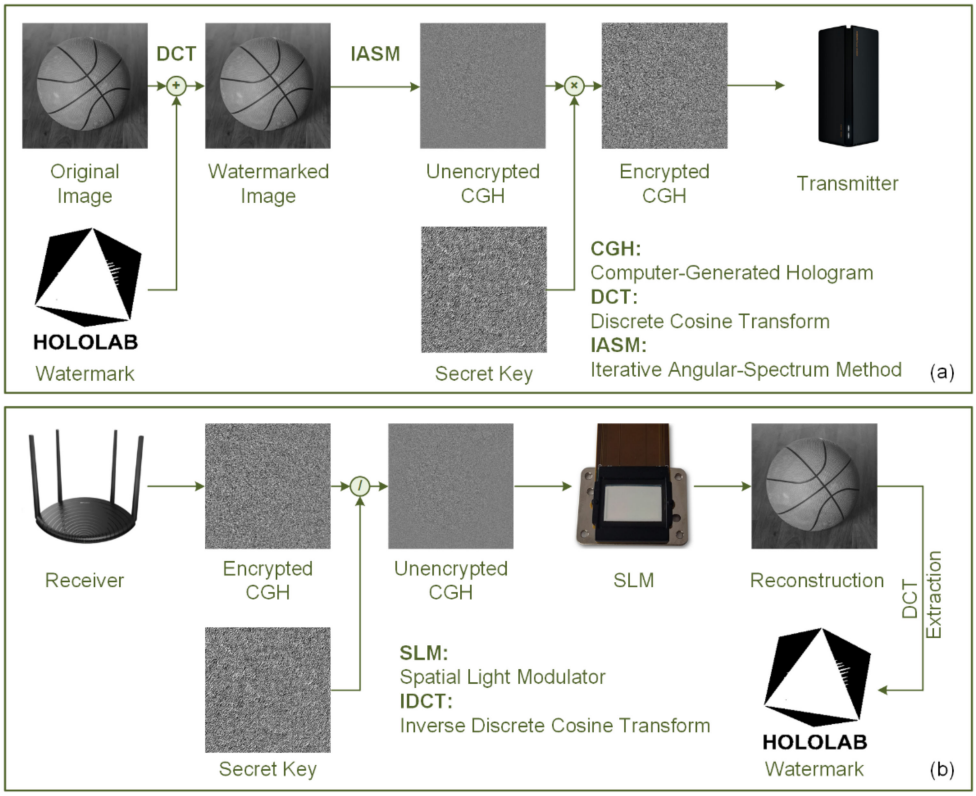

Figure 1. (**a**) The signal side and (**b**) the display side of the holographic communication system.

2.1. Insertion of the Watermark

The DCT-based insertion of the watermark is shown in Figure 2. For simplicity, the resolution of the original image is set as $M \times M$ pixels in this work. A binary image, with a resolution of $N \times N$ pixels, is employed as the watermark. Typically, the value of M/N is an integer. In the application of holographic communication, two critical issues should be considered during the watermark insertion: the invisibility of the watermark and the time efficiency of the insertion. The invisibility ensures that the inserted watermark does not occlude the displayed result, while the time efficiency ensures that the insertion does not bring time delay to the communication. DCT is a widely studied method in the field of watermark insertion. Through DCT, the image can be processed in the frequency domain, rather than the spatial domain. More importantly, the processing of high-frequency components in the frequency domain does not significantly affect the intensity distribution in the spatial domain. The invisibility of the watermark can easily be realized through the DCT-based insertion method [24,25]. Meanwhile, through parallel acceleration technology, the computational speed of the DCT-based insertion method can be guaranteed. Therefore, a DCT-based method together with parallel acceleration is employed in this work to insert the watermark.

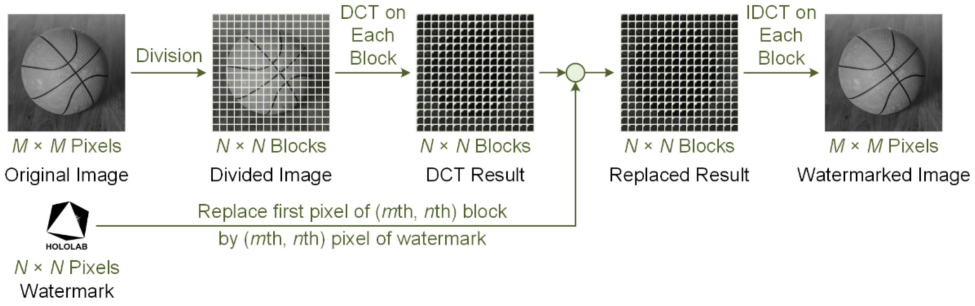

Figure 2. The DCT-based insertion of the watermark.

In this method, the original image is first divided into $N \times N$ blocks. DCT is then conducted on each block in parallel to obtain the distribution in the frequency domain, which can be expressed as:

$$E_{j,k}(m_1, n_1) = \mathrm{dct2}\left[I_{j,k}(m_1, n_1)\right] \tag{1}$$

where $I_{j,k}$ is the intensity distribution of the (jth, kth) block, $E_{j,k}$ is the frequency distribution of the (jth, kth) block, dct2 is the symbol of 2D-DCT, j and k are positive integers that do not exceed N, and m_1 and n_1 are positive integers that do not exceed M/N.

To realize the watermark insertion, the first pixel of $E_{j,k}$ is replaced by the (jth, kth) pixel of the watermark, which can be expressed as:

$$E'_{j,k}(m_1, n_1) = \begin{cases} E_{j,k}(m_1, n_1) \times [\beta + \alpha I_{wm}(j,k)], (m_1, n_1) = (1,1) \\ E_{j,k}(m_1, n_1), (m_1, n_1) \neq (1,1) \end{cases} \tag{2}$$

where I_{wm} is the intensity distribution of the watermark, $E'_{j,k}$ is the frequency distribution of the (jth, kth) block after the replacement of the pixels, and α and β are two scale factors. Finally, the watermarked image in the spatial domain can be recovered by the IDCT, which can be expressed as:

$$I'_{j,k}(m_1, n_1) = \mathrm{idct2}\left[E'_{j,k}(m_1, n_1)\right] \tag{3}$$

where $I'_{j,k}$ is the intensity distribution of the (jth, kth) block after the insertion of the watermark, and idct2 is the symbol of 2D inverse DCT (IDCT).

2.2. Calculation of the CGH

In conventional one-step computer-generated holography, the holographic reconstruction is always significantly affected by the noise. The irregularly distributed noise in the reconstructed image might disturb the frequency distribution obtained by DCT which makes the watermark difficult to extract. Therefore, a precise holographic algorithm is necessary to encode a watermarked image into a CGH. The iterative method that uses multiple forward and backward wavefront propagations with some constraints is often employed to encode a CGH with less noise [26–28]. Therefore, it is more suitable than the conventional one-step method to encode the CGH for a watermarked image.

In this work, an iterative method called IASM is employed, as shown in Figure 3. The IASM is formed via a forward propagation model and a backward propagation model. In the forward propagation model, the input amplitude is of uniform intensity, while the input phase is obtained from the backward propagation model. Considering that there is no calculation result from the backward propagation model during the first forward propagation, a random phase is employed as the initial input phase. The complex distribution on the holographic plane synthesized by the input amplitude and input phase is then processed through the ASM, which can be expressed as:

$$\widetilde{D}_{\mathrm{obj},\,p}(m,n) = \begin{cases} \mathrm{ifft2}\left\{\mathrm{fft2}\{\exp[\mathrm{i} \times 2\pi \times ran(m,n)]\} \times \exp\left[\mathrm{i}\frac{2\pi}{\lambda} z_0 \sqrt{1-(\lambda u_m)^2-(\lambda v_n)^2}\right]\right\}, \; p = 1 \\ \mathrm{ifft2}\left\{\mathrm{fft2}\left\{\exp\left[\mathrm{i} \times \arg\left(\widetilde{C}_{\mathrm{holo},p-1}(m,n)\right)\right]\right\} \times \exp\left[\mathrm{i}\frac{2\pi}{\lambda} z_0 \sqrt{1-(\lambda u_m)^2-(\lambda v_n)^2}\right]\right\}, \; p > 1 \end{cases} \tag{4}$$

where $\widetilde{D}_{obj}$ is the complex distribution on the object plane, $\widetilde{C}_{holo}$ is the complex distribution on the object plane, i is the symbol of the imaginary number, arg is the symbol of extracting the phase from the complex amplitude, p is the number of iterations, λ is the wavelength of the illumination wave, z_0 is the propagation distance, *ran* is a 2D real random matrix, fft2

and ifft2 are symbols of 2D fast Fourier transform (FFT) and 2D inverse FFT, and u_m and v_n are the discrete spatial frequencies that can be expressed as:

$$u_m = -\frac{1}{2\Delta} + \frac{m}{M\Delta}, v_n = -\frac{1}{2\Delta} + \frac{n}{M\Delta} \tag{5}$$

where Δ is the pixel pitch of the 2D matrix.

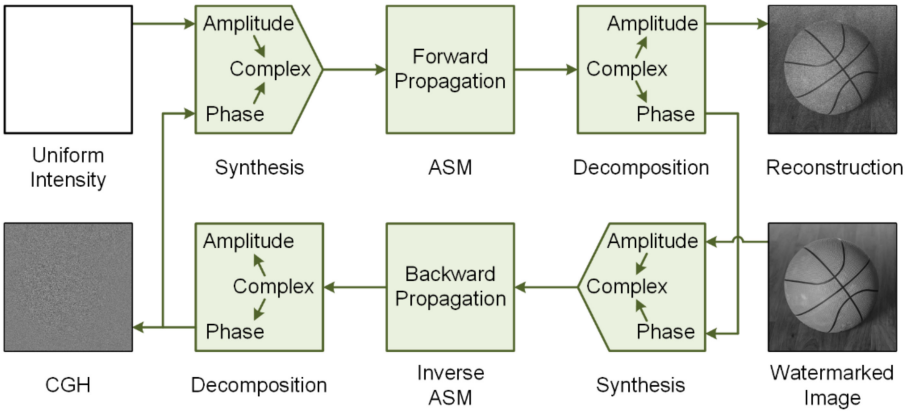

Figure 3. The calculation of the CGH by the IASM.

In the backward propagation model, the input amplitude is the watermarked image, while the input phase is obtained from the forward propagation model. The complex distribution on the object plane synthesized via the input amplitude and input phase is then processed by the inverse ASM, which can be expressed as:

$$\begin{aligned} \widetilde{C}_{\text{holo},p}(m,n) = \text{ifft2}\Big\{\text{fft2}\Big\{I'(m,n) \times \exp\Big[\text{i} \times \arg\Big(\widetilde{D}_{\text{obj},p}(m,n)\Big)\Big]\Big\} \\ \times \exp\Big[-\text{i} \times \tfrac{2\pi}{\lambda} z_0 \sqrt{1-(\lambda u_m)^2-(\lambda v_n)^2}\Big]\Big\} \end{aligned} \tag{6}$$

where I' is the entire watermarked image, which can be spliced by each block obtained from Equation (3). The optimized complex distribution can be obtained through repeating the forward and backward propagations described by Equations (5) and (6) until the number of iterations reaches a preset value p. The phase of the optimized complex distribution is finally extracted as the CGH for the watermarked image.

2.3. Encryption of the CGH

To enhance the confidentiality of the transmission, the obtained phase-only CGH should be encrypted. The process of encryption is shown in Figure 4. Firstly, a database for secret keys is established. Each secret key in the database is essentially a pseudo-random phase. To encrypt the phase-only CGH, a secret key located in row a and column b is selected. Then, the selected secret key is multiplied with the obtained CGH, generating an encrypted phase-only CGH, which can be expressed as:

$$H_{\text{encrypted}}(m,n) = \arg\Big[\widetilde{C}_{\text{holo},P}(m,n)\Big] * S_{a,b}(m,n) \tag{7}$$

where $\widetilde{C}_{\text{holo},p}$ is the complex distribution after p iterations, $S_{a,b}$ is the secret key located in row a and column b of the database, and * is the symbol of the element-wise product. To avoid the value of the matrix element in $H_{encrypted}$ being modulated to 0 by the secret key, the value of the matrix element in $S_{a,b}$ is never equal to 0. Additionally, to mark the location

of the selected secret key, the values of a and b are also encoded into the encrypted CGH, which can be expressed as:

$$H'_{\text{encrypted}}(m,n) = \begin{cases} \exp\left[\mathrm{i} \times \left(2\pi \times a/2^{D_{\text{bit}}} - \pi\right)\right], (m,n) = (1,1) \\ \exp\left[\mathrm{i} \times \left(2\pi \times b/2^{D_{\text{bit}}} - \pi\right)\right], (m,n) = (M,M) \\ H_{\text{encrypted}}(m,n), \text{others} \end{cases} \tag{8}$$

where D_{bit} is the bit depth of the encrypted CGH. In this work, the employed image always has a bit depth of 8 bits. Therefore, the maximal values of a and b can reach 256. This means that a database containing up to 256 × 256 secret keys can be established.

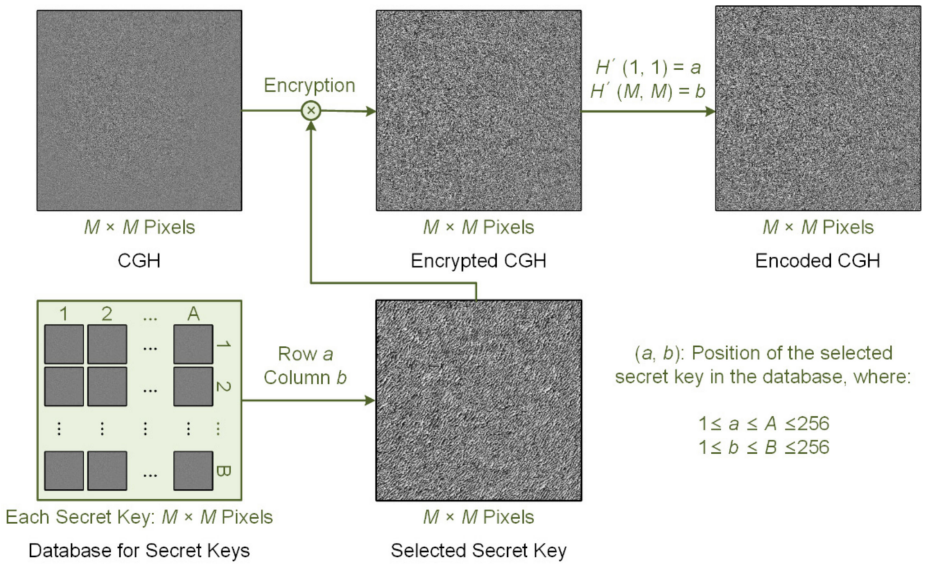

Figure 4. The encryption of the phase-only CGH before the transmission.

2.4. Reconstruction of the CGH

After being encrypted and encoded, the obtained phase distribution is transferred from the signal side to the display side using a transmitter and a receiver. A database that is totally the same as that in Figure 4 is also stored on the display side. To recover the phase-only CGH of the watermarked image, the location of the secret key that is employed to encrypt the CGH should be first searched, which can be expressed as:

$$I'_{\text{encrypted}}(m,n) = \frac{2^{D_{\text{bit}}} \times \left\{\arg\left[H'_{\text{encrypted}}(m,n)\right] + \pi\right\}}{2\pi} \tag{9}$$

$$a = I'_{\text{encrypted}}(1,1),\ b = I'_{\text{encrypted}}(M,M) \tag{10}$$

where $I'_{\text{encrypted}}$ is the normalized distribution extracted from $H'_{\text{encrypted}}$. By the coordinate value (a, b), the selected secret key $S_{a,b}$ can be easily found, being employed to decrypt the CGH, which can be expressed as:

$$H_{\text{unencypted}}(m,n) = H_{\text{encrypted}}(m,n)./S_{a,b}(m,n) \tag{11}$$

where / is the symbol of the element-wise division process. The decrypted CGH is then uploaded onto a phase-only CGH, optically reconstructing the watermarked image under the illumination of a coherent plane wave. Finally, the watermark inserted in the image can be extracted from the reconstructed image.

The extraction of the watermark is shown in Figure 5. The reconstructed watermarked image is divided into $N \times N$ blocks again. DCT is conducted on each block of the recon-

structed image in parallel to obtain the distribution in the frequency domain, which can be expressed as:

$$G_{j,k}(m_1, n_1) = \text{dct2}\left[R_{j,k}(m_1, n_1)\right] \tag{12}$$

where $R_{j,k}$ is the (jth, kth) block of the reconstructed image and $G_{j,k}$ is the frequency distribution of the (jth, kth) block. To realize the watermark extraction, the first pixel of $G_{j,k}$ is picked and processed, which can be expressed as:

$$I'_{wm}(j,k) = \left[G_{j,k}(1,1)/E_{j,k}(1,1) - \beta\right]/\alpha \tag{13}$$

where I'_{wm} is the extracted watermark. According to the information in the watermark, the source of the leak can easily be traced.

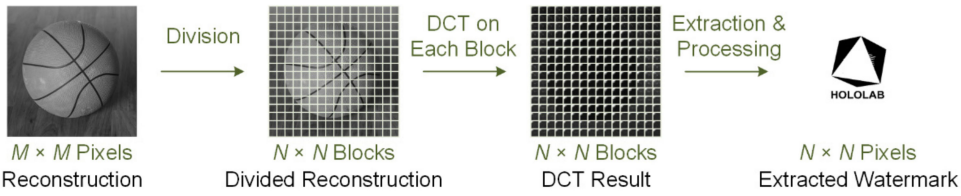

Figure 5. The extraction of the watermark from the optically reconstructed image.

3. Results

3.1. Numerical Experiments

To verify the effectiveness of the proposed watermarking and encryption for holographic communication, a series of simulations were conducted in this work. The images with a resolution of 2000 × 2000 pixels are employed as the original images, as shown in Figure 6a. A binary image shown in Figure 1a with a resolution of 250 × 250 pixels is employed as the watermark. The values of α, β, λ, z_0, Δ, and p are set as 0.02, 1, 532 nm, 150 mm, 3.74 μm, and 50, respectively. The database of the secret keys is formed by four pseudo-random phases.

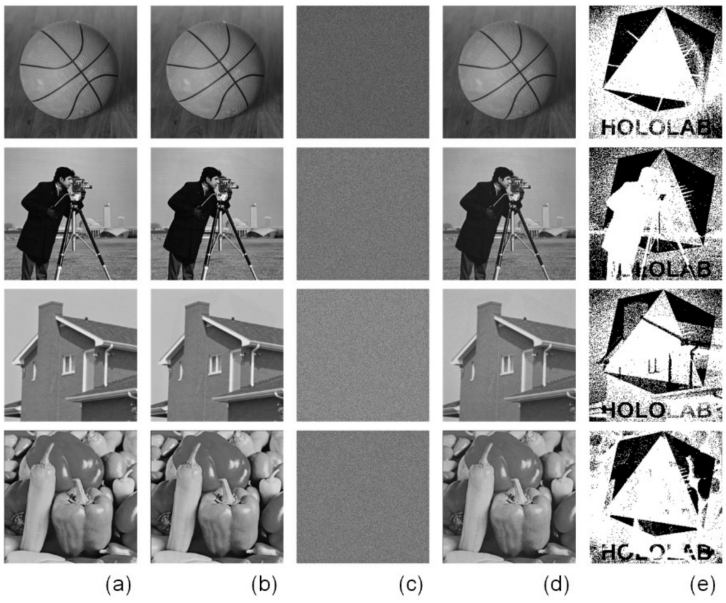

Figure 6. (**a**) The original images with a resolution of 2000 × 2000 pixels. (**b**) The watermarked images. (**c**) The reconstructions of encrypted CGHs. (**d**) The reconstructions of decrypted CGHs. (**e**) The extracted watermarks from the reconstructions.

The watermarked images obtained via the method described in Section 2.1 are shown in Figure 6b. It can be observed from the results that the invisibility of the watermark is

well-satisfied by employing the mentioned parameters. In addition, the time consumption of inserting the watermark into an original image can be reduced to 0.19 s by using parallel computation, presenting prominent applicability in holographic communication. When the encrypted CGHs are employed in the holographic reconstruction, the reconstructed images are shown in Figure 6c. Obviously, when the secret keys are not used to decrypt CGHs, the reconstructed images cannot be recognized. If the scale of the secret key database is large enough, it would be more difficult to recover the distributions of secret keys, making it significantly hard to decrypt the CGHs without permission. The reconstructed images by using decrypted CGHs are shown in Figure 6d. By applying IASM in the calculation of CGHs, displayed images with shape details and suppressed noises are readily obtained. To extract watermarks from the displayed images, the method mentioned in Section 2.4 is applied. The extracted watermarks are shown in Figure 6e. It can be seen from the results that if the encrypted signal is decrypted by non-target users, the source of the leak can also be easy to trace.

3.2. Optical Experiments

To further verify the effectiveness of the proposed watermarking and encryption method, a practical holographic communication system was established. The transmitter and receiver used in the system are a Xiaomi CR6609 router and a TP-Link AC1200 router, respectively. After receiving the encrypted CGHs, a notebook (Xiaomi Notebook Pro 15) is employed to process these CGHs and upload them onto an SLM. The SLM is placed in a holographic display system, which is shown in Figure 7a. A laser with a wavelength of 532 nm is employed as the illumination of the system. The illumination beam passes through an attenuator, a pinhole, and a polarizer and then is collimated with a convex lens. The collimated beam illuminates the SLM, being modulated by the CGH uploaded on it. Finally, the reconstructed wave is reflected via a beam splitter and is captured with a camera (Canon 60D).

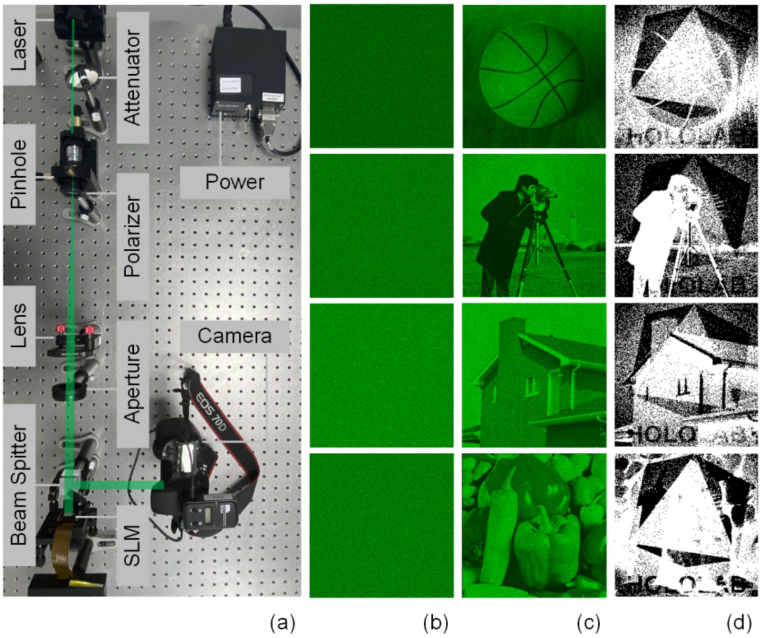

Figure 7. (**a**) The optical experimental system. (**b**) The reconstructions of encrypted CGHs. (**c**) The reconstructions of decrypted CGHs. (**d**) The extracted watermarks from the reconstructions.

The reconstructions of encrypted CGHs and decrypted CGHs are shown in Figure 7b,c, respectively. To promote the image quality of holographic reconstructions, the look-up table (LUT) of the SLM was corrected in advance [29]. Like the results in numerical experiments, the reconstructions can only be recognized when CGHs have been decrypted. As shown

in Figure 7d, by applying the watermark extraction method described in Section 2.4, the inserted watermark can be readily recovered, making it easier to trace the source of the leak when the displayed images are captured without permission. Therefore, the watermarking and encryption method is functional in optical experiments. Through this method, the signal can be encrypted and watermarked in holographic communication, which can be used to protect the privacy and copyright in future applications.

4. Discussion

4.1. Effect of Scale Factors

As mentioned in Equation (2), α and β are two scale factors during the watermark insertion. When the value of α remains unchanged (α = 0.02), the watermarked images under different values of β are shown in Figure 8a. It can be seen from the results that the brightness of the watermarked image increases with the value of β. When the value of β is closer to 1, the brightness of the watermarked image is closer to the original image. When the decrypted CGHs are used, the reconstructions of watermarked images under different values of β are shown in Figure 8b. Correspondingly, the watermarks extracted from these reconstructions are shown in Figure 8c. Obviously, the image quality of the extracted watermark gradually decreases with the value of β.

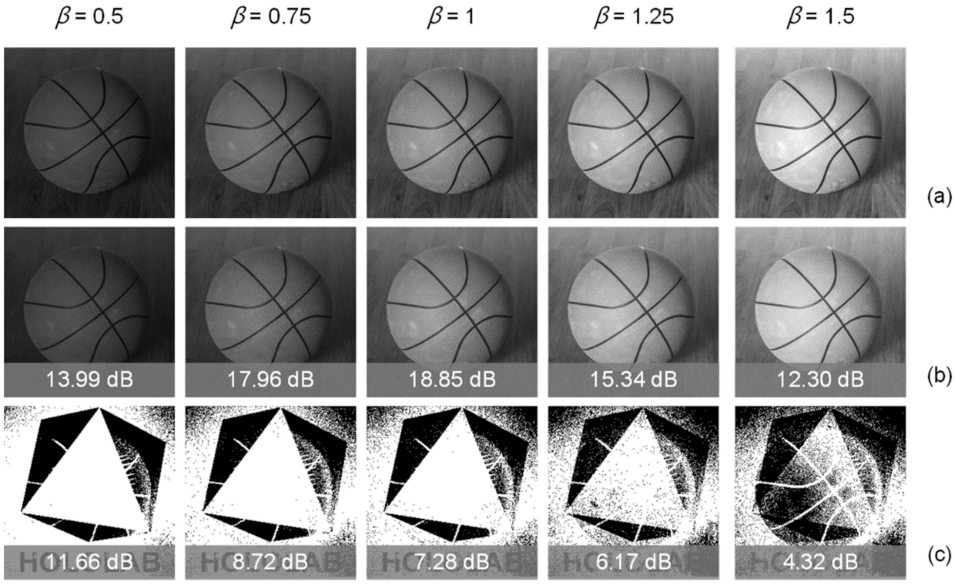

Figure 8. (**a**) The watermarked images with different values of β. (**b**) The reconstructions of decrypted CGHs. (**c**) The extracted watermarks from the reconstructions.

To quantitatively evaluate the image quality of holographic reconstructions and the extractability of watermarks, the peak signal-to-noise ratio (PSNR) was employed. As shown in Figure 8b,c, the PSNR of the holographic reconstruction reaches its maximal value when the value of β is 1, while the PSNR of the extracted watermark decreases with the value of β. By adjusting the value of β, the image quality of holographic reconstructions and the extractability of the watermarks can be satisfied simultaneously.

In addition to the effect of β, the influence caused by the value of α is also explored. When the value of β remains unchanged (β = 1), the watermarked images under different values of α are shown in Figure 9a. It can be seen from the results that the visibility of the watermark increases with the value of α. When the decrypted CGHs are used, the reconstructions of watermarked images under different values of α are shown in Figure 9b. Correspondingly, the watermarks extracted from these reconstructions are shown in Figure 9c. The PSNR of the holographic reconstruction decreases with the value of α by a small degree, which means that the image quality of the holographic reconstruction deteriorates slowly. However, the visibility of the watermark increases

dramatically. Considering the results of Figures 8 and 9 together, it can be concluded that the image quality of the extracted watermark improves with the value of α/β. Although there is no limit on α and β, setting the values of α and β as 0.02 and 1 might be a reasonable choice when both the visibility and extractability of the watermark are considered.

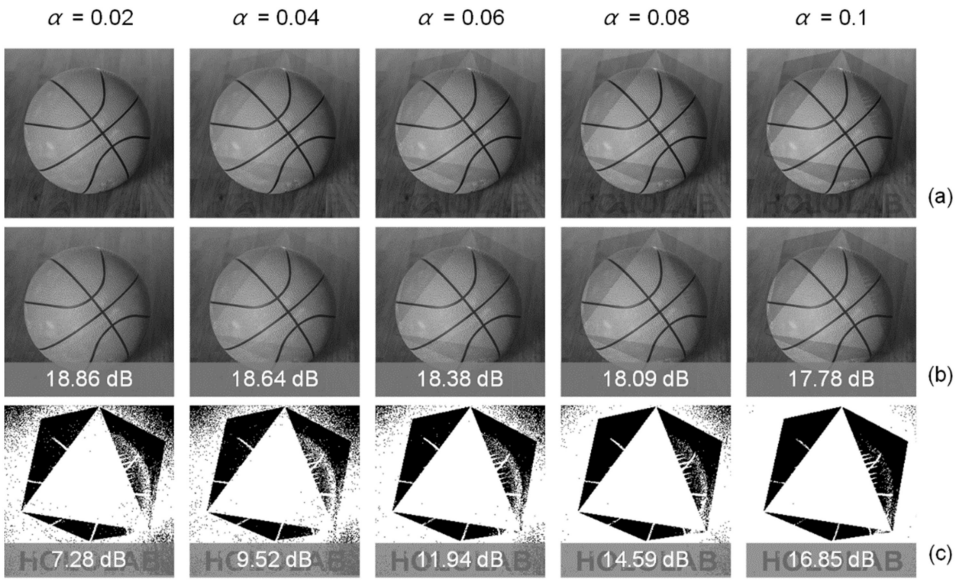

Figure 9. (**a**) The watermarked images with different values of α. (**b**) The reconstructions of decrypted CGHs. (**c**) The extracted watermarks from the reconstructions.

4.2. Effect of Iteration-Based Optimization

As mentioned in Section 2.2, the holographic reconstruction is often affected by the noise in conventional one-step computer-generated holography. Being influenced by the noise, the image quality of the holographic display is significantly limited, while the extraction of the watermark from the reconstruction is difficult. To address this issue, the IASM is employed. The reconstructions and extracted watermarks under different iteration numbers p are shown in Figure 10. It can be seen from the results that speckle noise in the reconstruction by a one-step CGH is plainly observed. The watermark extracted from the reconstruction is extremely fuzzy. With the increase in the iteration number p, the speckle noise can be suppressed. The clarity of the extracted watermark is improved. However, when the iteration number is larger than 20, the density of speckles in the reconstruction and the clarity of the extracted watermark see little improvement with the increase in the iteration number. This trend can also be seen in the change in the PSNR value. Considering the consumption of the computing power, 20 iterations might be an optional choice in most cases.

4.3. Robustness

To measure the robustness of the proposed watermarking and encryption method, some typical noises, including Gaussian noise, speckle noise, salt and pepper noise, and occlusion, are introduced into the encrypted CGHs. The CGHs under different introduced noises are shown in Figure 11a. When the encrypted CGHs are decrypted and reconstructed, holographic reconstructions and their locally enlarged results are shown in Figure 11b,c, respectively. Correspondingly, the watermarks extracted from these reconstructions are shown in Figure 11d.

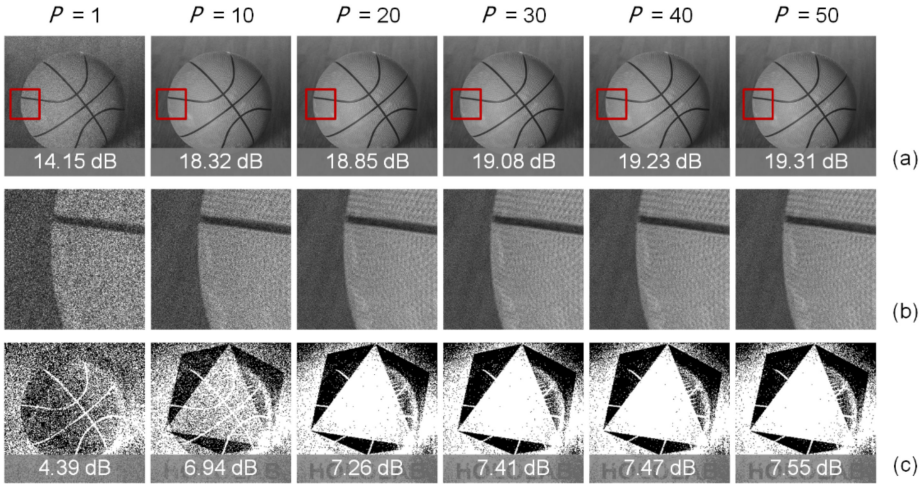

Figure 10. (**a**) Holographic reconstructions under different iteration numbers. (**b**) Locally enlarged results of holographic reconstructions. (**c**) The extracted watermarks from the reconstructions.

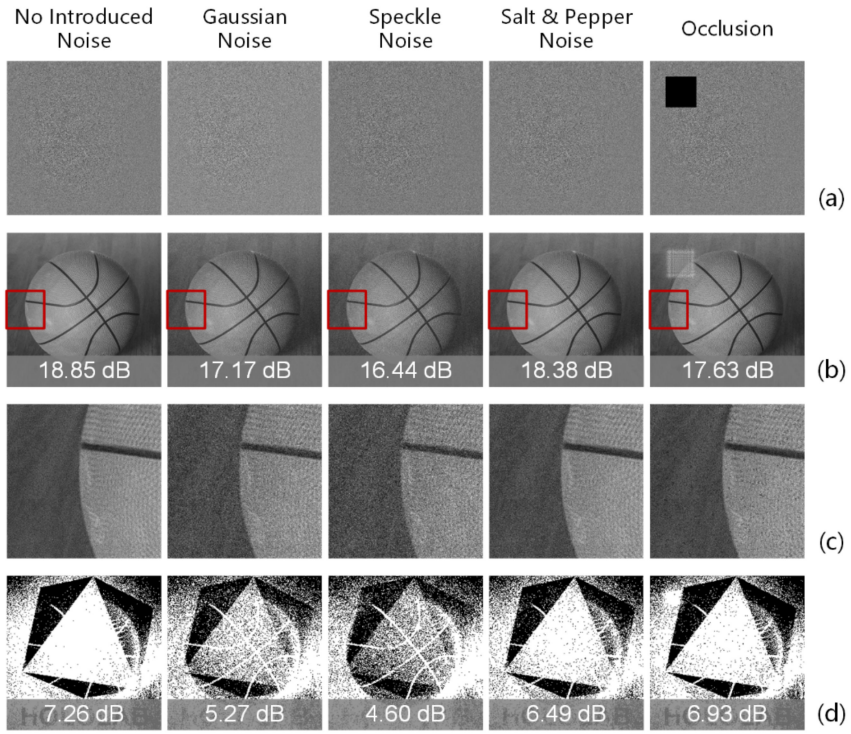

Figure 11. (**a**) CGHs under different introduced noises. (**b**) Holographic reconstructions under different introduced noises. (**c**) Locally enlarged results of holographic reconstructions. (**d**) The extracted watermarks from the reconstructions.

It can be seen from the results that the image quality of holographic reconstructions is obviously influenced by the introduced noises. The decline in the PSNR caused by the Gaussian noise or speckle noise is more severe than that caused by salt and pepper noise or occlusion. However, even if the image quality of holographic reconstructions is obviously influenced by these introduced noises, the inserted watermarks can still be easily extracted from the reconstructed images. Therefore, the proposed watermarking and encryption method shows its reliability in holographic communication.

5. Conclusions

In this work, a watermarking and encryption method for holographic communication is proposed. In this method, the original image to be presented is first watermarked via the DCT-based insertion strategy. The precise CGH of the watermarked image is then calculated by the IASM. To encrypt the obtained CGH, a secret key selected from the database is employed. The location of the secret key is also encoded into the encrypted CGH. The time consumption of inserting the watermark into the original image can be reduced to 0.19 s by using parallel computation, presenting a prominent applicability in holographic communication. The reconstruction of the encrypted CGH can only be recognized when the correct secret key is employed. If the scale of the secret key database is large enough, it would be difficult to recover the distributions of secret keys, making it significantly hard to decrypt the CGHs without permission. Even if the encrypted signal is decrypted by non-target users, the source of the leak can also be easy to trace by extracting the inserted watermark from the holographic reconstruction.

The proposed watermarking and encryption method provides an optional solution for the privacy protection and copyright protection of holographic communication. In our future work, the concealment and robustness of the watermark will be improved; the effectiveness of the watermark insertion for full-color 3D images will be studied; the acceleration strategy for precise phase-only CGHs will be explored; and a secret key that is more difficult to decrypt will be designed.

Author Contributions: Conceptualization, Z.H.; data curation, Z.H.; formal analysis, Z.H.; funding acquisition, Z.H. and L.C.; investigation, Z.H. and K.L.; methodology, Z.H.; project administration, Z.H. and L.C.; resources, Z.H. and K.L.; software, Z.H.; supervision, L.C.; validation, Z.H.; visualization, Z.H.; writing—original draft, Z.H.; writing—review and editing, Z.H. and L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Postdoctoral Program for Innovative Talents, grant number BX2021140; National Natural Science Foundation of China (NSFC), grant number 62035003.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Orts-Escolano, S.; Rhemann, C.; Fanello, S.; Chang, W.; Kowdle, A.; Degtyarev, Y.; Kim, D.; Davidson, P.L.; Khamis, S.; Dou, M.; et al. Holoportation: Virtual 3D Teleportation in Real-Time. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology, Tokyo, Japan, 16–19 October 2016.
2. Gotsch, D.; Zhang, X.; Merritt, T.; Vertegaal, R. TeleHuman2: A Cylindrical Light Field Teleconferencing System for Life-Size 3D human Telepresence. In Proceedings of the 2018 CHI Conference on Human Factors in Computing System, Montreal, QC, Canada, 21–26 April 2018.
3. Lawrence, J.; Goldman, D.B.; Achar, S.; Blascovich, G.M.; Desloge, J.G.; Fortes, T.; Gomez, E.M.; Häberling, S.; Hoppe, H.; Huibers, A.; et al. Project Starline: A high-fidelity telepresence system. *ACM Trans. Graph.* **2021**, *40*, 242. [CrossRef]
4. He, Z.; Sui, X.; Jin, G.; Cao, L. Progress in virtual reality and augmented reality based on holographic display. *Appl. Opt.* **2019**, *58*, A74–A81. [CrossRef] [PubMed]
5. He, Z.; Sui, X.; Cao, L. Holographic 3D display using depth maps generated by 2D-to-3D rendering approach. *Appl. Sci.* **2021**, *11*, 9889. [CrossRef]
6. He, Z.; Sui, X.; Zhang, H.; Jin, G.; Cao, L. Frequency-based optimized random phase for computer-generated holographic display. *Appl. Opt.* **2021**, *60*, A145–A154. [CrossRef]
7. Liu, K.; He, Z.; Cao, L. Pattern-adaptive error diffusion algorithm for improved phase-only hologram generation. *Chin. Opt. Lett.* **2021**, *19*, 050501. [CrossRef]
8. He, Z.; Sui, X.; Jin, G.; Cao, L. Distortion-correction method based on angular spectrum algorithm for holographic display. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6162–6169. [CrossRef]

9. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
10. Zhang, Y.; Wang, B. Optical image encryption based on interference. *Opt. Lett.* **2008**, *33*, 2443–2445. [CrossRef]
11. Tsang, P.W.M.; Poon, T.C.; Cheung, K.W.K. Fast numerical generation and encryption of computer-generated Fresnel holograms. *Appl. Opt.* **2011**, *50*, 46–52. [CrossRef]
12. Wang, X.; Zhao, D. Optical image hiding with silhouette removal based on the optical interference principle. *Appl. Opt.* **2012**, *51*, 686–691. [CrossRef]
13. Chen, W.; Chen, X. Security-enhanced interference-based optical image encryption. *Opt. Commun.* **2013**, *286*, 123–129. [CrossRef]
14. Cai, J.; Shen, X.; Lei, M.; Lin, C.; Dou, S. Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition. *Opt. Lett.* **2015**, *40*, 475–478. [CrossRef]
15. Kong, D.; Cao, L.; Jin, G.; Javidi, B. Three-dimensional scene encryption and display based on computer-generated holograms. *Appl. Opt.* **2016**, *55*, 8296–8300. [CrossRef]
16. Kong, D.; Cao, L.; Shen, X.; Zhang, H.; Jin, G. Image encryption based on interleaved computer-generated holograms. *IEEE Trans. Ind. Inform.* **2018**, *14*, 673–678. [CrossRef]
17. Barni, M.; Bartolini, F.; Piva, A. Improved wavelet-based watermarking through pixel-wise masking. *IEEE Trans. Image Process.* **2001**, *10*, 783–791. [CrossRef]
18. Agreste, S.; Puccio, L. Wavelet-based watermarking algorithms: Theory, applications and critical aspects. *Int. J. Comput. Math.* **2011**, *88*, 1885–1895. [CrossRef]
19. Horng, S.-J.; Rosiyadi, D.; Fan, P.; Wang, X.; Khan, M.K. An adaptive watermarking scheme for e-government document images. *Multimed. Tools Appl.* **2014**, *72*, 3085–3103. [CrossRef]
20. Wang, C.-Y.; Kong, X.-W.; Li, C. Process color watermarking: The use of visual masking and dot gain correction. *Multimed. Tools Appl.* **2017**, *76*, 16291–16314.
21. Liu, J.; Rao, Y.; Huang, Y. Complex wavelet-based image watermarking with the human visual saliency model. *Electronics* **2019**, *8*, 1462. [CrossRef]
22. Kumari, R.; Mustafi, A. An optimized framework for digital watermarking based on multi-parameterized 2D-FrFT using PSO. *Optik* **2021**, *248*, 168077. [CrossRef]
23. He, Z.; Sui, X.; Jin, G.; Chu, D.; Cao, L. Optimal quantization for amplitude and phase in computer-generated holography. *Optics Express* **2021**, *29*, 119–133. [CrossRef]
24. Hamidi, M.; Haziti, M.E.; Cherifi, H.; Hassouni, M.E. Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. *Multimed. Tools Appl.* **2018**, *77*, 27181–27214. [CrossRef]
25. Ernawan, F.; Kabir, M.N. A robust image watermarking technique with an optimal DCT-psychovisual threshold. *IEEE Access* **2018**, *6*, 20464–20480. [CrossRef]
26. Sun, P.; Chang, S.; Liu, S.; Tao, X.; Wang, C.; Zheng, Z. Holographic near-eye display system based on double-convergence light Gerchberg-Saxton algorithm. *Opt. Express* **2018**, *26*, 10140–10151. [CrossRef]
27. Kim, H.; Kim, M.; Lee, W.; Ahn, J. Gerchberg-Saxton algorithm for fast and efficient atom rearrangement in optical tweezer traps. *Opt. Express* **2019**, *27*, 2184–2196. [CrossRef]
28. Wu, Y.; Wang, J.; Chen, C.; Liu, C.-J.; Jin, F.-M.; Chen, N. Adaptive weighted Gerchberg-Saxton algorithm for generation of phase-only hologram with artifacts suppression. *Opt. Express* **2021**, *29*, 1412–1427. [CrossRef]
29. Li, R.; Gao, Y.; Cao, L. In situ calibration for a phase-only spatial light modulator based on digital holography. *Opt. Eng.* **2020**, *59*, 053101. [CrossRef]