electronics

MDPI

Article

Enhanced Three-Dimensional Double Random Phase Encryption: Overcoming Phase Information Loss in Zero-Amplitude Singularities for Simultaneous Two Primary Data

Myungjin Cho [1,*] and Min-Chul Lee [2,*]

[1] School of ICT, Robotics, and Mechanical Engineering, IITC, Hankyong National University, 327 Chungang-ro, Anseong 17579, Republic of Korea
[2] Graduate School of Computer Science Systems Engineering, Kyushu Institute of Technology, 680-4 Kawazu, Iizuka-shi 820-8502, Fukuoka, Japan
* Correspondence: mjcho@hknu.ac.kr (M.C.); lee@csn.kyutech.ac.jp; (M.-C.L.)

Abstract

This paper proposes an advanced three-dimensional optical encryption technique based on double random phase encryption for the simultaneous encryption of two primary datasets. While conventional double random phase encryption offers high-speed encryption, it suffers from low data efficiency. To address this issue, the proposed method assigns the first primary dataset to the amplitude and the second to the phase. However, this approach faces a critical limitation: the phase information becomes undefined or lost when the amplitude is zero. Therefore, we introduce a biased amplitude encoding scheme for double random phase encryption to ensure the mathematical recoverability of the phase component. In the proposed method, a biased value ϵ is added to the amplitude part during the double random phase encryption encryption process and subsequently subtracted from the decrypted data to recover the two primary datasets. To verify the effectiveness of our approach, we employ synthetic aperture integral imaging and volumetric computational reconstruction. The experimental results show that while the first dataset remains lossless, the lossy characteristics of the second dataset are significantly mitigated.

Keywords: double random phase encryption; phase information; biased amplitude encoding

1. Introduction

In the modern digital era, protecting private information has become a critical necessity across various industries. Optical encryption has emerged as a powerful solution due to its inherent advantages, such as high processing speeds, operating at the speed of light, and the ability to handle multi-dimensional data. Among various optical techniques, double random phase encryption (DRPE) [1–13] is widely recognized as a foundational approach. DRPE employs a $4f$ optical system in which the primary data are encrypted using two independent random phase masks located in the spatial and spatial frequency domains, respectively. Decryption is possible only when the complex conjugate of the second random phase mask is provided as a security key.

While conventional DRPE is effective, its security can be compromised if the key is exposed. To enhance the security level, researchers have incorporated photon-counting imaging [14,15], which limits the number of photons in the encrypted data, making it unrecognizable to the human eye even if the key is known. Furthermore, the transition from two-dimensional (2D) to three-dimensional (3D) encryption [16] has been facilitated

Check for updates

Academic Editor: Aryya Gangopadhyay

Received: 29 January 2026
Revised: 13 February 2026
Accepted: 18 February 2026
Published: 22 February 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

by integral imaging [17–26], a technique first proposed by G. Lippmann. By using synthetic aperture integral imaging (SAII) [22], multiple elemental images can be recorded from different perspectives. These images are then processed using volumetric computational reconstruction (VCR) [27,28] to reconstruct 3D images at a specific reconstruction depth (z_r). This depth serves as an additional and robust security key, since the primary data becomes clear only when reconstructed at the correct longitudinal position.

Despite these advancements, a persistent challenge in DRPE-based systems is low data efficiency. In a standard $4f$ system, DRPE typically encrypts only one primary dataset into a single complex-valued encrypted set. In 3D imaging systems that require dozens or even hundreds of elemental images, the data burden becomes immense; for example, transmitting 100 elemental images at 4K resolution could require approximately 5 GB of data. To address this issue, recent studies have proposed a simultaneous encryption technique that assigns two different primary datasets to the amplitude and phase of a single input signal [29]. By treating the first dataset as the amplitude (I_1) and the second as the phase (I_2), the system effectively doubles data efficiency, enabling two images to be transmitted within the same capacity as one.

However, critical mathematical and physical limitations are revealed in this simultaneous approach: while the first primary data, which is assigned to the amplitude component of the signal during the encryption process, can be reconstructed almost perfectly, the second primary data, which is assigned to the phase component of the signal during the encryption process, is inherently lossy. This discrepancy occurs because the phase component is a periodic function (with a 2π period) and its accurate recovery strictly depends on the existence of non-zero-amplitude values. Specifically, when the first dataset is zero or near zero, the second dataset, which is assigned to the phase component of the signal, is lost or becomes undefined, leading to significant reconstruction noise.

In this paper, we propose a novel solution to the zero-amplitude singularity problem. By introducing a modified encoding algorithm, we ensure that the phase information remains recoverable regardless of the intensity of the primary amplitude data. The following sections present the proposed biased encoding method, the integration of SAII and VCR for 3D security, and experimental results demonstrating improved peak signal-to-noise ratio (PSNR), structural similarity index measure (SSIM), and peak sidelobe ratio (PSR) values for the lossy phase component.

2. Principle of Double Random Phase Encryption

Double random phase encryption (DRPE) is a cornerstone of optical security, valued for its ability to process information at the speed of light through optical components. The system primarily operates in a $4f$ optical configuration, employing two independent random phase masks (RPMs) to convert primary data into stationary white noise.

2.1. Encryption Process

The encryption is implemented using a $4f$ optical system consisting of two lenses with a focal length f, as illustrated in Figure 1. The process follows these sequential steps. The first step is spatial domain encoding. The primary data, denoted as $s(x)$, are first multiplied by the first RPM, $\exp\{i2\pi n_s(x)\}$, in the spatial domain, where $n_s(x)$ is a random phase generated from a uniform distribution within the range [0, 1]. The second step is Fourier transform. The encoded signal then passes through Lens 1, which performs a Fourier Transform to generate a spatial frequency spectrum at the focal plane. The third step is frequency domain encoding. At this focal plane, the spectrum is multiplied by a second RPM, $\exp\{i2\pi n_f(\mu)\}$, where $n_f(\mu)$ is also a random phase uniformly distributed between

0 and 1. The final step is inverse Fourier transform. The signal passes through Lens 2, performing an inverse Fourier transform to produce the encrypted data $s_e(x)$.

Mathematically, the encryption process is defined as [1]

$$s_e(x) = \mathcal{F}^{-1}\left[\mathcal{F}\left\{s(x)e^{i2\pi n_s(x)}\right\}e^{i2\pi n_f(\mu)}\right] \quad (1)$$

The resulting encrypted data $s_e(x)$ are complex-valued, consisting of both amplitude and phase components, neither of which can be visually recognized without the proper decryption key.

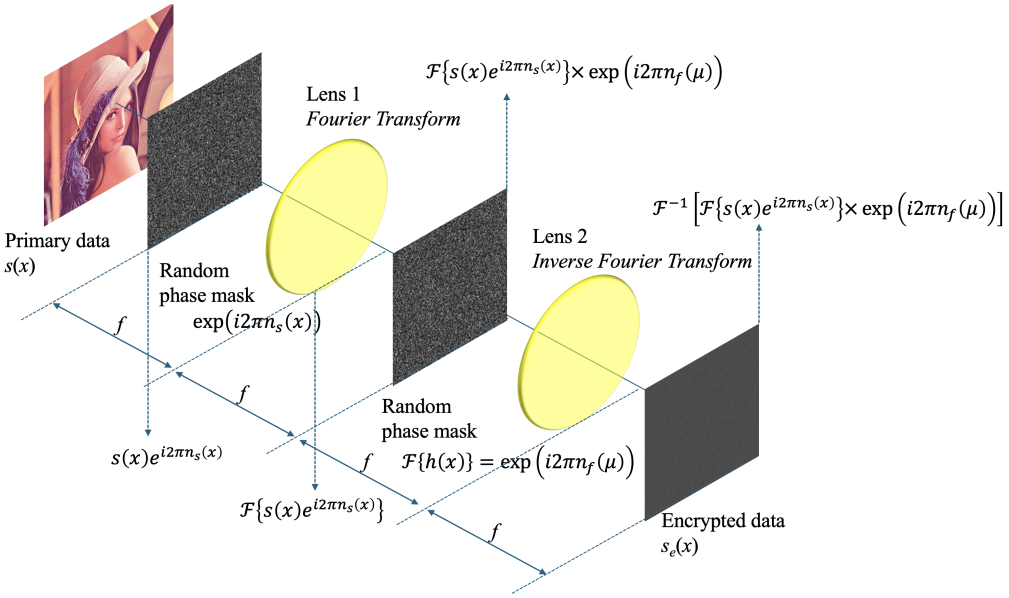


Figure 1. Encryption process of double random phase encryption.

2.2. Decryption Process

Figure 2 illustrates the decryption process of DRPE. Decryption requires a homogeneous $4f$ optical system and a security key, which is the complex conjugate of the second RPM used during encryption, $\exp\{-2\pi n_f(\mu)\}$.

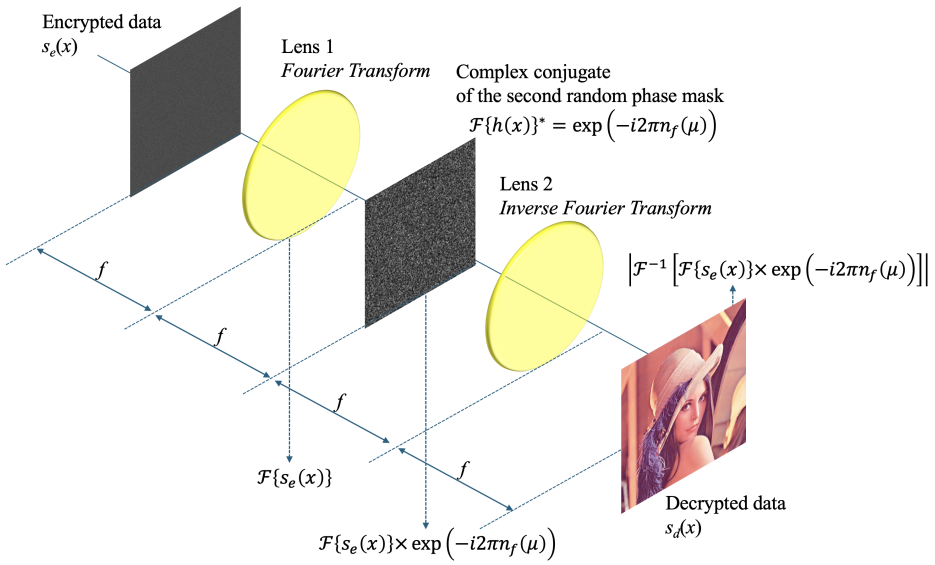


Figure 2. Decryption process of double random phase encryption. Here, the superscript * indicates the complex conjugate of $\mathcal{F}\{h(x)\}$.

The decryption process proceeds through these sequential steps. The first step is Fourier transform of ciphertext. The encrypted data $s_e(x)$ are transformed by Lens 1 into the spatial frequency domain. The second step is key multiplication. The spectrum is multiplied by the complex conjugate of the second RPM, $\exp\{-i2\pi n_f(\mu)\}$, which serves as the key information. The third step is inverse Fourier transform. Lens 2 performs an inverse Fourier transform to return the signal to the spatial domain. The final step is intensity detection. An image sensor captures the result by taking the absolute value of the decrypted signal, $s_d(x)$.

The decryption is expressed as [1]

$$s_d(x) = \left| \mathcal{F}^{-1}\left[\mathcal{F}\{s_e(x)\} \times e^{-i2\pi n_f(\mu)} \right] \right| \tag{2}$$

If the correct key is provided, the primary data are reconstructed perfectly, resulting in a mean squared error (MSE) of zero. However, if the key is incorrect or unknown, the output appears as unrecognizable noisy images, as shown in Figure 3.

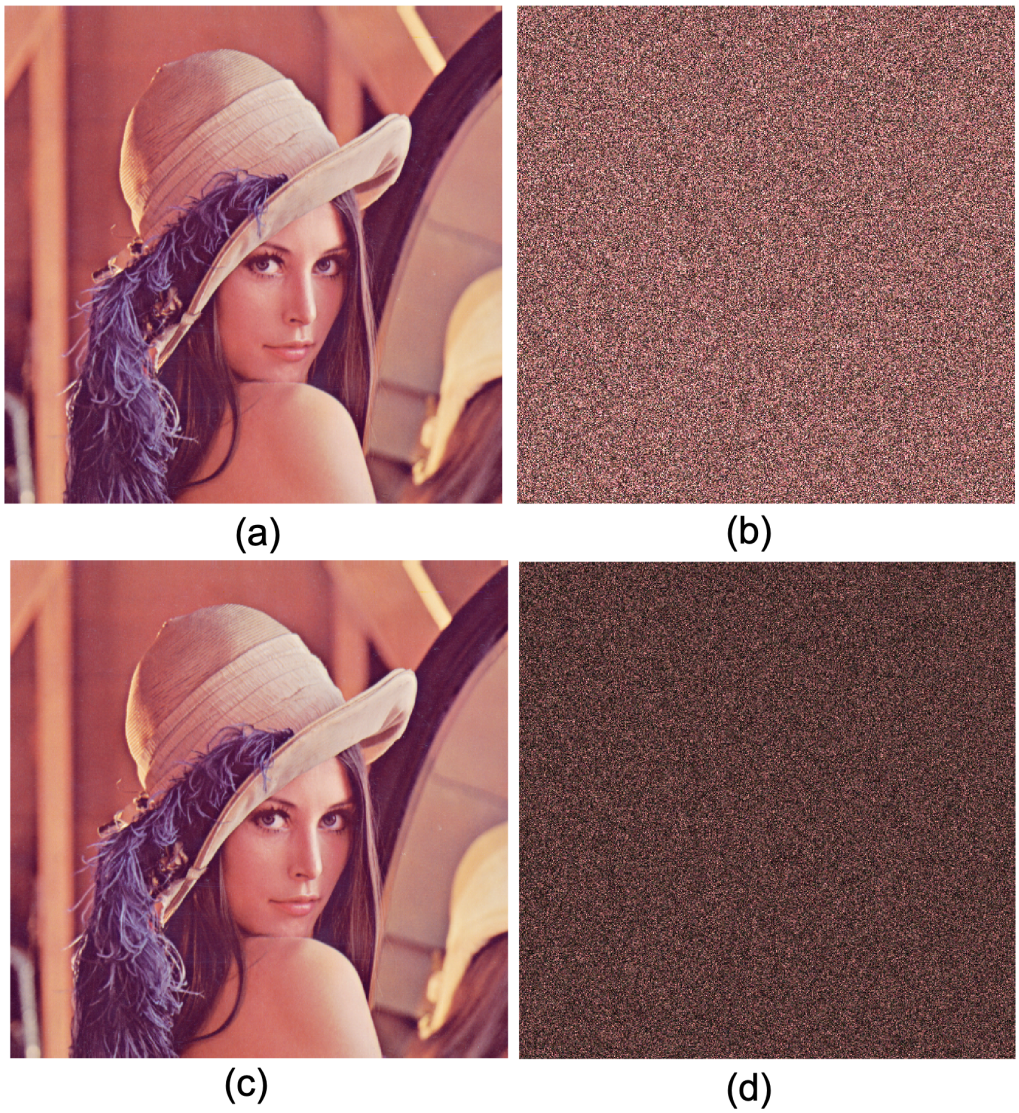


Figure 3. Examples of double random phase encryption: (**a**) primary data, (**b**) encrypted data, (**c**) decrypted data with correct key, and (**d**) decrypted data with incorrect key.

2.3. Limitations of Conventional DRPE

Despite its advantages in speed and security, several critical drawbacks are identified in the conventional approach. The first issue is security vulnerability. If the key random phase mask is exposed, the data can be easily decrypted by unauthorized parties. The second issue is low data efficiency. Traditionally, DRPE encrypts only one primary dataset into a single encrypted set, which becomes problematic for 3D imaging systems (e.g., integral imaging) that require transmitting large amounts of data, such as 100 elemental images exceeding 5 GB at 4 K resolution. The third issue involves phase reconstruction. The phase component of the decrypted data may not be accurately reconstructed because it is a periodic function with a 2π period. This problem is particularly evident when the amplitude reaches zero, as the phase information becomes difficult to recover accurately. These limitations—specifically, the lossy nature of the phase component and the need for higher data efficiency—motivate the development of the simultaneous two primary data encryption method [29].

3. Three-Dimensional Double Random Phase Encryption for Simultaneous Two Primary Data

In this section, we present the acquisition of 3D information using synthetic aperture integral imaging and simultaneous two primary data encryption algorithm.

3.1. Acquisition of 3D Information via SAII

To record high-resolution 3D information, we employ synthetic aperture integral imaging (SAII). Unlike conventional lens array based systems, in which the resolution is limited by the number of lenses, SAII records elemental images by moving a single camera or by using a camera array. This process captures multiple perspectives of a 3D object, where each elemental image I_{kl} (corresponding to the kth column and ith row) possesses high resolution. In this study, 9(H) $\times$ 9(V) elemental images were captured for each primary dataset, providing the necessary spatial information for robust 3D reconstruction.

3.2. Simultaneous Two Primary Data Encryption Algorithm

The core of our proposal is to improve data efficiency, which is traditionally low in DRPE because a single primary dataset typically corresponds to one encrypted set. To double the data efficiency, we combine two distinct primary datasets—the first dataset $I_1(x)$ and the second dataset $I_2(x)$—into a single complex input.

The encryption process follows these steps illustrated in Figure 4. The first step is amplitude and phase assignment. The first primary dataset $I_1(x)$ is assigned as the amplitude, while the second primary dataset $I_2(x)$ is converted into a phase-type signal, $\exp\{i2\pi I_2(x)\}$. The second step is Fourier transform. The combined signal passes through Lens 1, performing a Fourier transform. The third step is frequency domain encoding. The resulting spectrum is multiplied by the second random phase mask, $\exp\{i2\pi n_f(\mu)\}$. The final step is inverse Fourier transform. Lens 2 performs an inverse Fourier transform to produce the encrypted data, as expressed in [29]

$$\hat{s}_e(x) = \mathcal{F}^{-1}\left[\mathcal{F}\left\{I_1(x)e^{i2\pi I_2(x)}\right\}e^{i2\pi n_f(\mu)}\right] \tag{3}$$

Using this method, a pair of images—for example, a 512 $\times$ 512-pixel color text image and a 512 $\times$ 512-pixel color test image—can be encrypted into a single set of complex-valued data, reducing the transmission capacity from 3.2 MB to 1.6 MB. Figure 5 shows the encrypted data obtained through DRPE for the simultaneous encryption of two primary

datasets. As shown in Figure 5c,f, two primary datasets can be encrypted simultaneously into a single encrypted output.

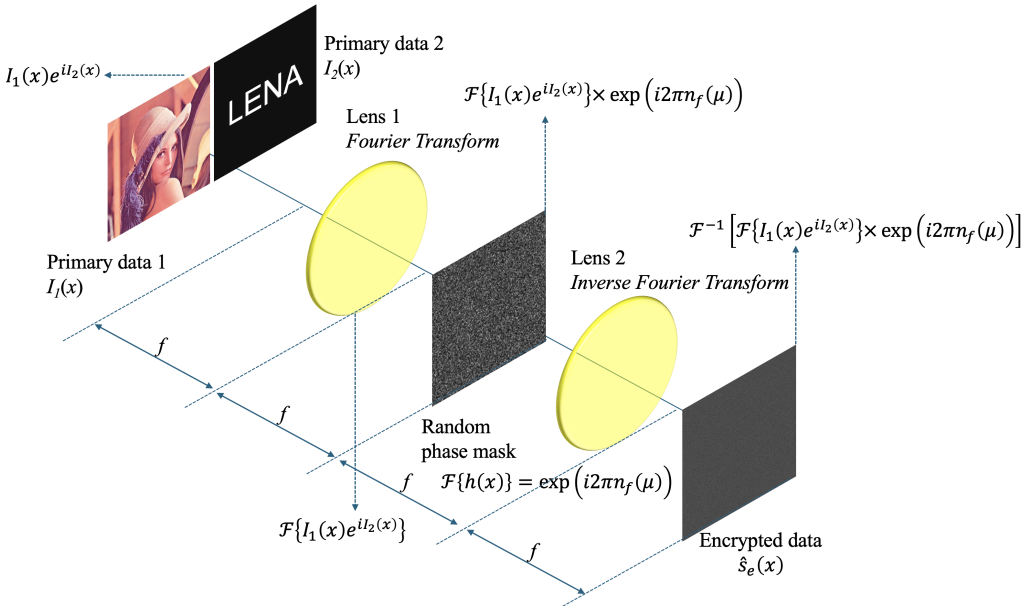


Figure 4. Encryption process of DRPE for simultaneous two primary data.

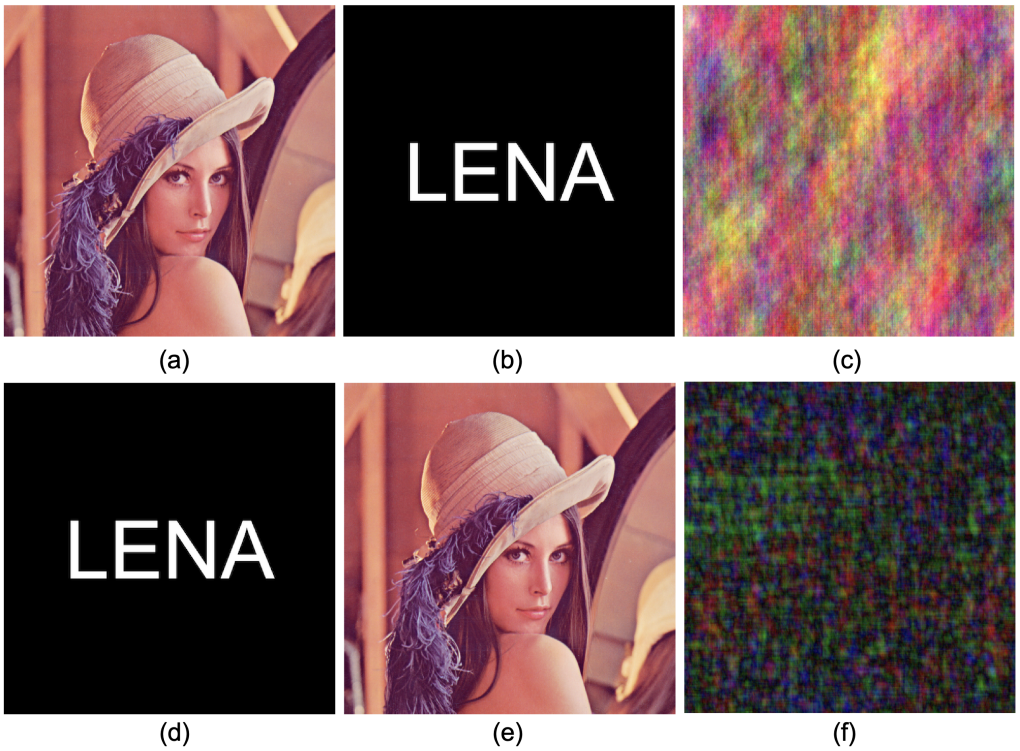


Figure 5. Encryption examples of DRPE for simultaneous two primary data: (**a**) primary data 1, (**b**) primary data 2, (**c**) encrypted data for (**a**,**b**), (**d**) primary data 1, (**e**) primary data 2, and (**f**) encrypted data for (**d**,**e**).

3.3. Decryption and Separation of Simultaneous Data

Figure 6 illustrates the decryption process of DRPE for simultaneous encryption of two primary datasets. Decryption requires the complex conjugate of the second random phase mask, $\exp\{-i2\pi n_f(\mu)\}$. After multiplying the encrypted data by this key and performing an inverse Fourier transform, the decrypted signal $\hat{s}_d(x)$ is obtained as in [29]

$$\hat{s}_d(x) = \mathcal{F}^{-1}\left[\mathcal{F}\{\hat{s}_e(x)\} \times e^{-i2\pi n_f(\mu)}\right] \tag{4}$$

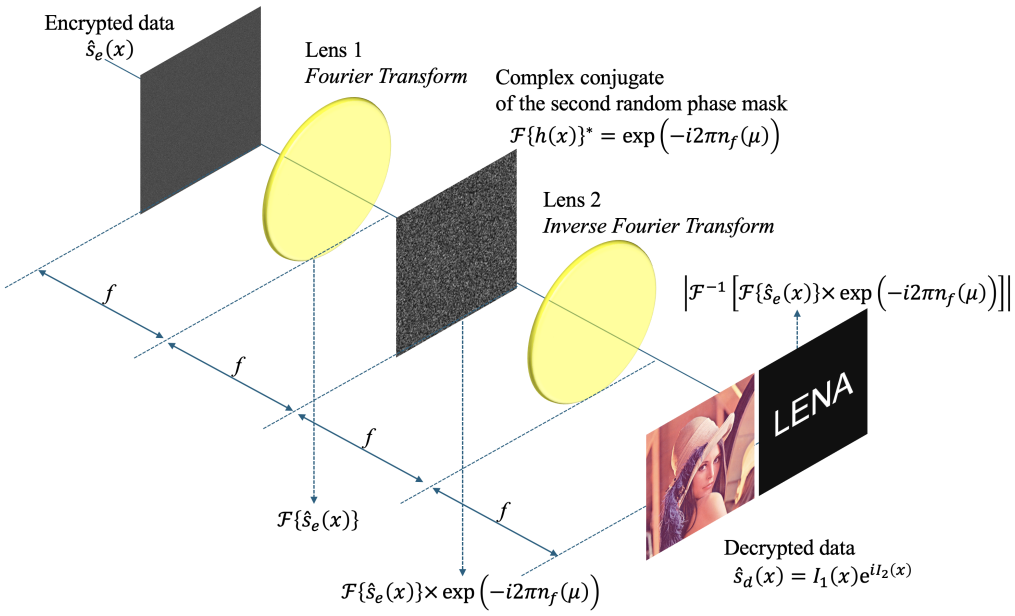


Figure 6. Decryption process of DRPE for simultaneous two primary data. Here, the superscript * indicates the complex conjugate of $\mathcal{F}\{h(x)\}$.

The two datasets are separated as follows [29]:

$$\hat{I}_1(x) = |\hat{s}_d(x)| \tag{5}$$

$$\hat{I}_2(x) = \frac{\mathrm{mod}(\angle \hat{s}_d(x), 2\pi)}{2\pi} \tag{6}$$

Figure 7 shows the decrypted results of DRPE for the simultaneous encryption of two primary dataset. The two primary datasets shown in Figure 7a,b are correctly decrypted from the encrypted data in Figure 5c. In contrast, while one primary dataset in Figure 7c is correctly decrypted, the other dataset in Figure 7d fails to decrypt properly from the encrypted data in Figure 5f, because the first primary dataset shown in Figure 5d contains zero values that cause the zero-amplitude singularity. Consequently, the decrypted dataset in Figure 7d may be lost.

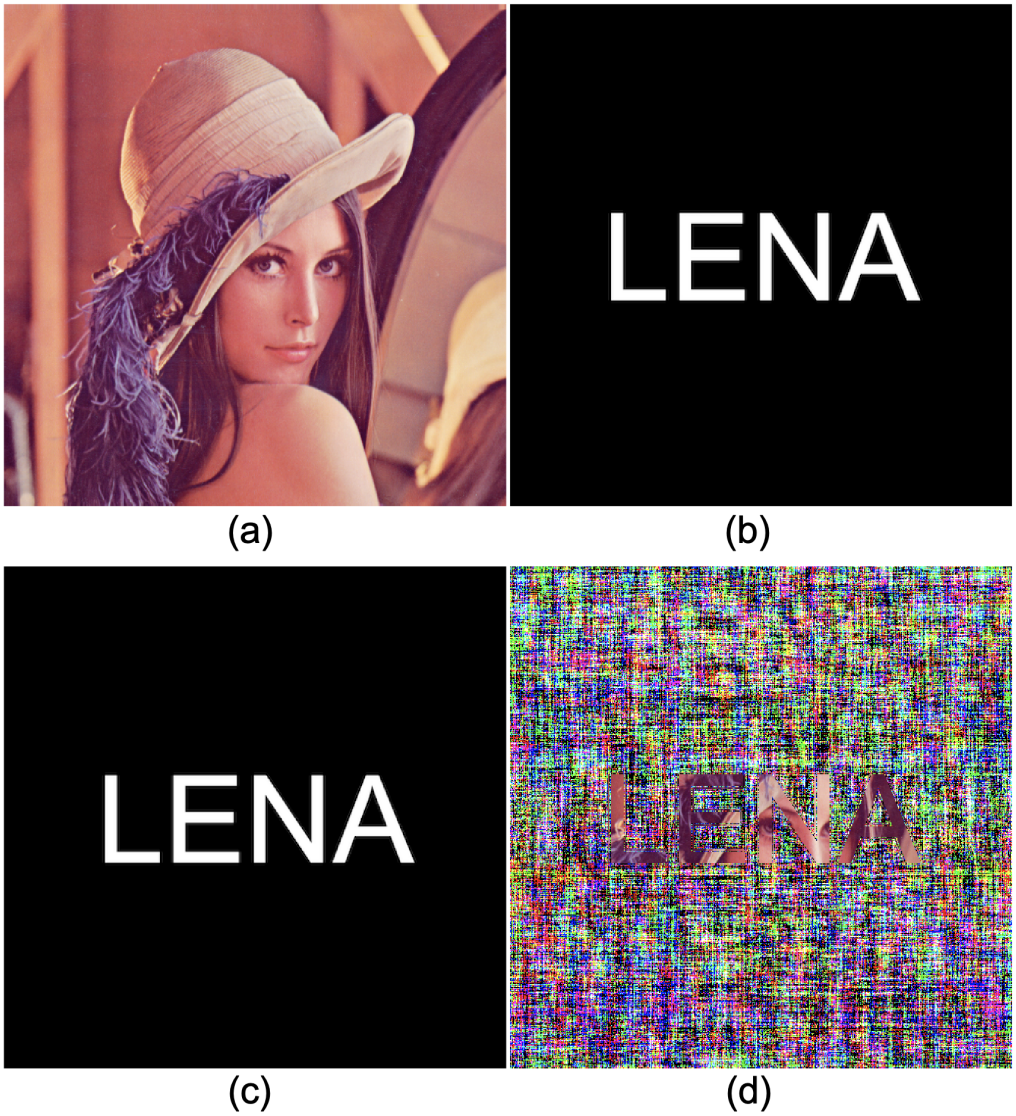


Figure 7. Zero-amplitude singularity in decryption of conventional DRPE for simultaneous two primary data. (**a**) data 1 from encrypted data in Figure 5c, (**b**) data 2 from encrypted data in Figure 5c, (**c**) data 1 from encrypted data in Figure 5f, and (**d**) data 2 from encrypted data in Figure 5f.

4. Proposed Solution for Phase Information Loss (Biased Encoding)

In this section, we describe the encryption process, decryption, and separation of simultaneous data in the proposed method.

4.1. Encryption Process of Our Method

A significant drawback identified in DRPE for the simultaneous encryption of two primary datasets is that the phase component of the decrypted data may not be reconstructed accurately because the phase is a periodic function with a 2π period. Specifically, when the amplitude $I_1(x)$ becomes zero, the phase information $I_2(x)$ becomes mathematically undefined, making the second primary dataset inherently lossy.

To address this issue, we propose biased amplitude encoding. A small constant bias ϵ is added to the first primary dataset to ensure that $I_1(x) > 0$ at all coordinates as shown in Figure 8.

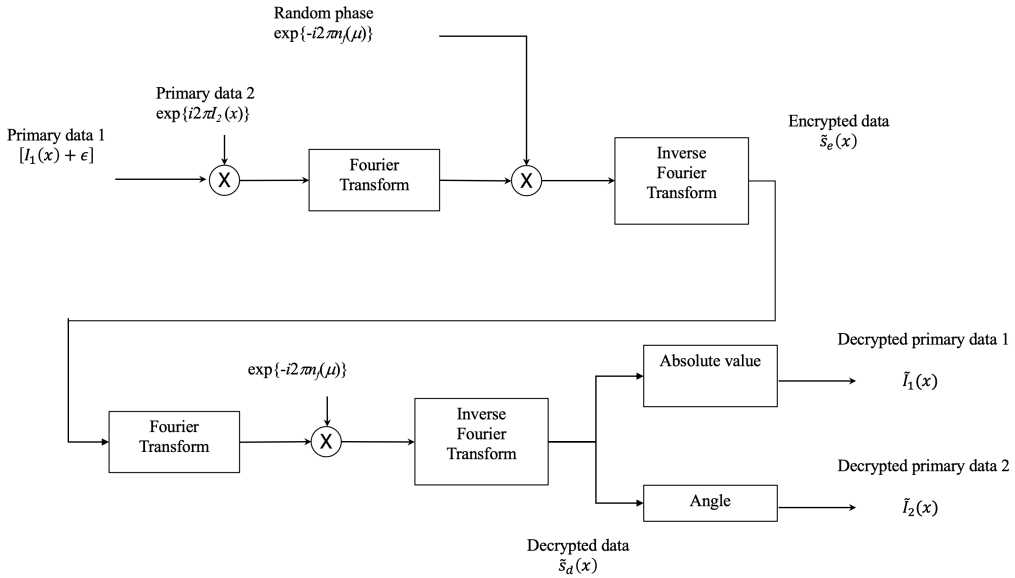


Figure 8. Proposed DRPE for simultaneous two primary data.

The encrypted data, $\tilde{s}_e(x)$, generated by our method is expressed as:

$$\tilde{s}_e(x) = \mathcal{F}^{-1}\left[\mathcal{F}\left\{[I_1(x) + \epsilon]e^{i2\pi I_2(x)}\right\}e^{i2\pi n_f(\mu)}\right] \tag{7}$$

This modification ensures that the vector magnitude never becomes zero, allowing the angle to be precisely calculated during decryption and thereby mitigating the lossy nature of the second primary dataset.

4.2. Decryption and Separation of Biased Simultaneous Data

Decryption requires the complex conjugate of the second random phase mask, $\exp\{-i2\pi n_f(\mu)\}$. After multiplying the encrypted data by this key and performing an inverse Fourier transform, the decrypted signal $\tilde{s}_d(x)$ is obtained, as shown in Figure 8. The decryption process is expressed as:

$$\tilde{s}_d(x) = F^{-1}\left[F\{\tilde{s}_e(x)\} \times e^{-i2\pi n_f(\mu)}\right] \tag{8}$$

The two datasets are separated as follows:

$$\tilde{I}_1(x) = |\tilde{s}_d(x)| - \epsilon \tag{9}$$

$$\tilde{I}_2(x) = \frac{\mathrm{mod}(\angle[\tilde{s}_d(x) - \epsilon], 2\pi)}{2\pi} \tag{10}$$

Figure 9 shows the encrypted and decrypted data obtained using our method, where a constant bias $\epsilon = 0.1$ is applied. It can be observed that both primary datasets are accurately decrypted.

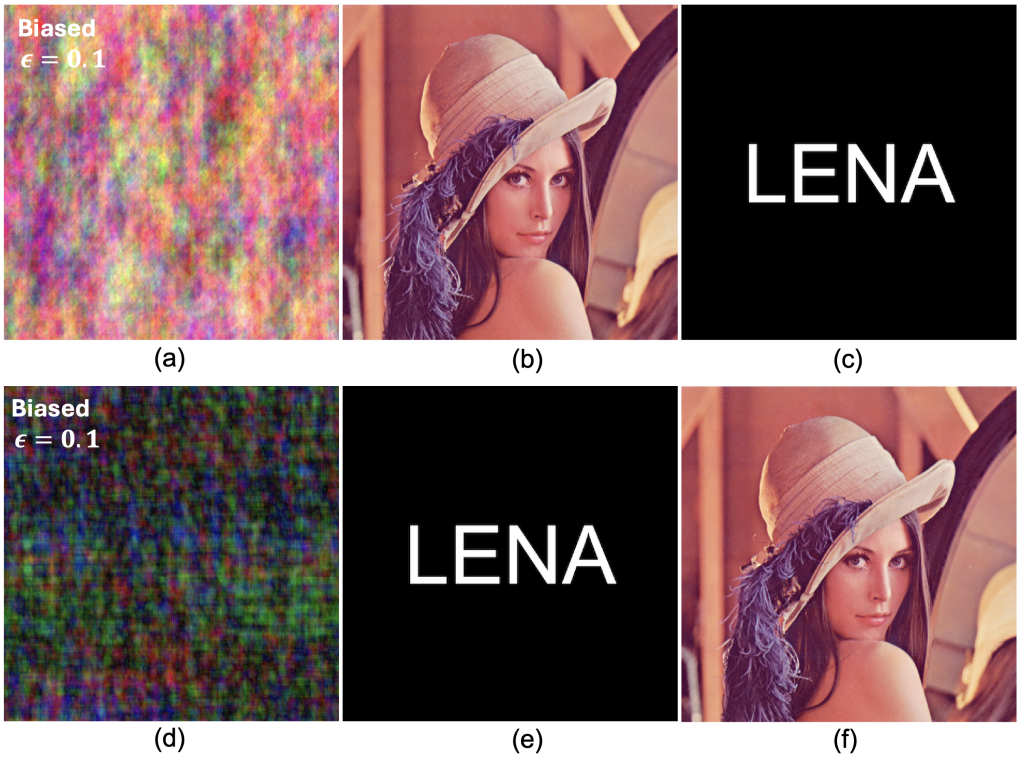


Figure 9. Examples by our method. (**a**) encrypted data for simultaneous two primary data with a constant bias of $\epsilon = 0.1$, (**b**) data 1 for (**a**), (**c**) data 2 for (**a**), (**d**) encrypted data for simultaneous two primary data with a constant bias of $\epsilon = 0.1$, (**e**) data 1 for (**d**), (**f**) data 2 for (**d**).

4.3. 3D Volumetric Computational Reconstruction (VCR)

Finally, the decrypted elemental images are reconstructed into 3D space using volumetric computational reconstruction (VCR) [27,28] as illustrated in Figure 10. VCR projects elemental images through a virtual pinhole array onto a reconstruction plane at depth z_r. The images are then shifted by Δx and Δy as described in [28]:

$$\Delta x = \frac{N_x f p_x}{c_x z_r}, \quad \Delta y = \frac{N_y f p_y}{c_y z_r} \tag{11}$$

where N_x, Ny denote the number of pixels in each elemental image, f is the focal length of the camera, p_x, p_y are the camera pitches, c_x, c_y represent the image sensor size, the subscripts x, y indicate the directions, and z_r is the reconstruction depth.

The final 3D reconstructed images, $\tilde{I}_1(x, y, z_r)$ and $\tilde{I}_2(x, y, z_r)$, are obtained by averaging the overlapping pixels, as described in Equation (12) [28]. This averaging operation further helps suppress decryption noise. In the proposed method, the reconstruction depth (z_r) acts as a secondary security key, since objects appear in focus only at their correct longitudinal positions.

$$\tilde{I}_n(x, y, z_r) = \frac{1}{O(x, y, z_r)} \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} \tilde{I}_{nkl}(x + \lceil \Delta x \times k \rfloor, y + \lceil \Delta y \times l \rfloor) \tag{12}$$

where n is the index of the primary data; $O(x, y, z_r)$ is the overlapping matrix at the reconstruction depth z_r; k, l are the indices of the elemental images; $\lceil \cdot \rfloor$ denotes the rounding operator; and K, L represent the total number of elemental images in the x and y directions, respectively.

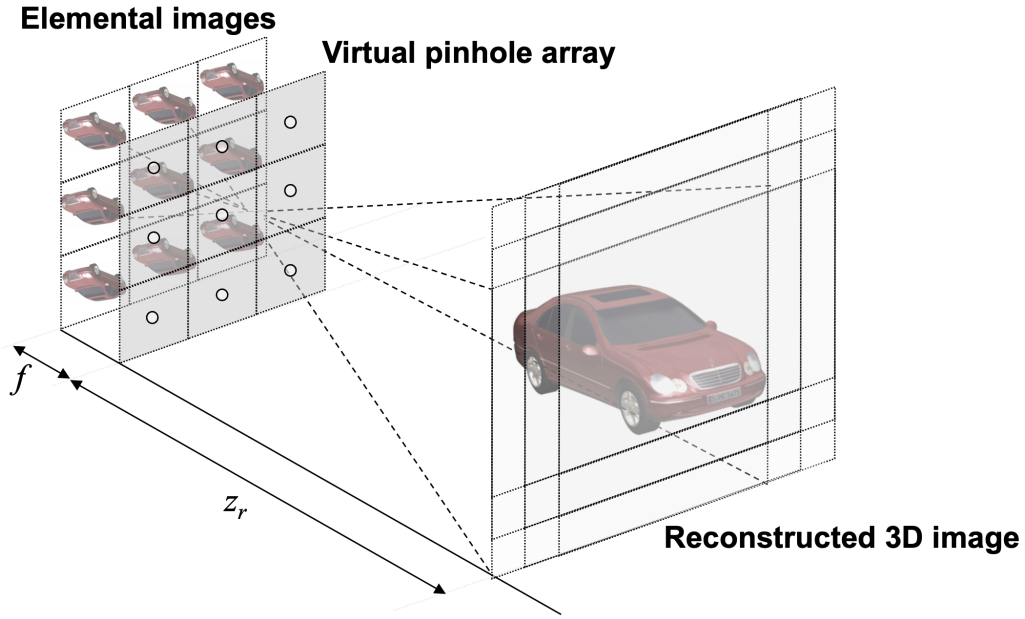


Figure 10. Concept of volumetric computational reconstruction.

5. Experimental Results and Discussion

To verify the feasibility of the proposed biased encoding method and evaluate its impact on 3D simultaneous encryption, we conducted a series of computational experiments.

5.1. Experimental Environment and Parameters

We utilized a synthetic aperture integral imaging (SAII) system to obtain high-resolution elemental images. The experimental parameters were configured as follows. The camera array consists of $9(H) \times 9(V)$ virtual cameras and the image resolution of each elemental image is 512×512 pixels. The first pair of primary datasets comprises the "LENA" text image and the Lena test image, as shown in Figure 11. The second pair comprises the "MANDRILL" text image and the Mandrill test image, as shown in Figure 12. The focal length of the camera, f, is 50 mm, sensor size, c_x and c_y, is 36 mm $\times$ 36 mm, and the camera pitch, p, is 7.2 mm. The test objects for the first primary dataset (I_1)—the "LENA" and "MANDRILL" text images with black backgrounds—are placed at a reconstruction depth of 512 mm. For the second primary dataset (I_2), the corresponding Lena and Mandrill test images are positioned at a reconstruction depth of 1024 mm. To implement the proposed method numerically, a MacBook Pro 2018 (Intel Core i7 2.6 GHz, 32 GB memory, and Intel UHD Graphics 630) and MATLAB R2024b were used.

Figure 13 shows the decryption results of the conventional DRPE for the simultaneous encryption of two primary datasets (i.e., without applying a constant bias, ϵ). It is evident that the second primary dataset cannot be decrypted accurately using this method. In contrast, the decryption results obtained with our proposed method (i.e., with a constant bias of $\epsilon = 0.1$) are accurately reconstructed, as shown in Figure 14. These results demonstrate that the proposed method can successfully encrypt and decrypt two primary datasets without loss of the second dataset.

Figures 15 and 16 show the 3D reconstruction results obtained using our method. Since the text images are located at $z_r = 512$ mm and test images are located at $z_r = 1024$ mm, only the 3D reconstructions at their corresponding depths appear clear. This indicates that the reconstruction depth can serve as additional key information in our DRPE method.



Figure 11. Elemental images for (**a**) LENA text and (**b**) Lena image.

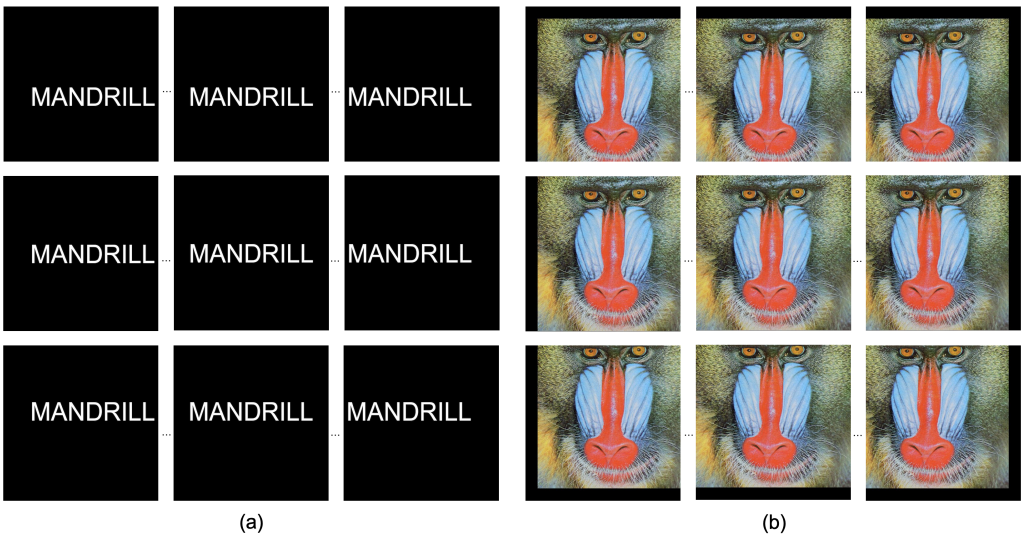


Figure 12. Elemental images for (**a**) MANDRILL text and (**b**) Mandrill image.

5.2. Performance Metrics: PSNR and PSR

To evaluate the quality of the decrypted data and the accuracy of the 3D reconstruction, we employed two primary metrics. The peak signal-to-noise ratio (PSNR) and the structural similarity index measure (SSIM) were used to assess the fidelity of the 2D decrypted images relative to the original data. Moreover, the peak sidelobe ratio (PSR) was calculated using a k-th law nonlinear correlation filter (e.g., k = 0.3) [30] to determine the sharpness of the reconstruction at various depths. A high PSR peak at the correct depth z_r indicates successful 3D volumetric reconstruction.

5.3. Analysis of 2D Decryption Results

In the conventional simultaneous encryption scheme without a constant bias ϵ, the first primary dataset is lossless, achieving an extremely high PSNR of 57.1856 dB and an SSIM of 0.9995. However, the second primary dataset (the phase-encoded image) is lossy, with a PSNR of 8.2346 dB and an SSIM of 0.0665 for the Lena dataset. For the Mandrill dataset, the first primary dataset shows a high PSNR of 55.8164 dB and an SSIM of 0.9993, whereas the second dataset exhibits a low PSNR of 8.2869 dB and an SSIM of 0.0460 due to the zero-amplitude singularity. This loss occurs because the phase component cannot be

reconstructed accurately owing to its periodic nature. Specifically, in the black background regions of the "LENA" and "MANDRILL" text images—where the amplitude is zero—the phase information of the second test images is mathematically destroyed.

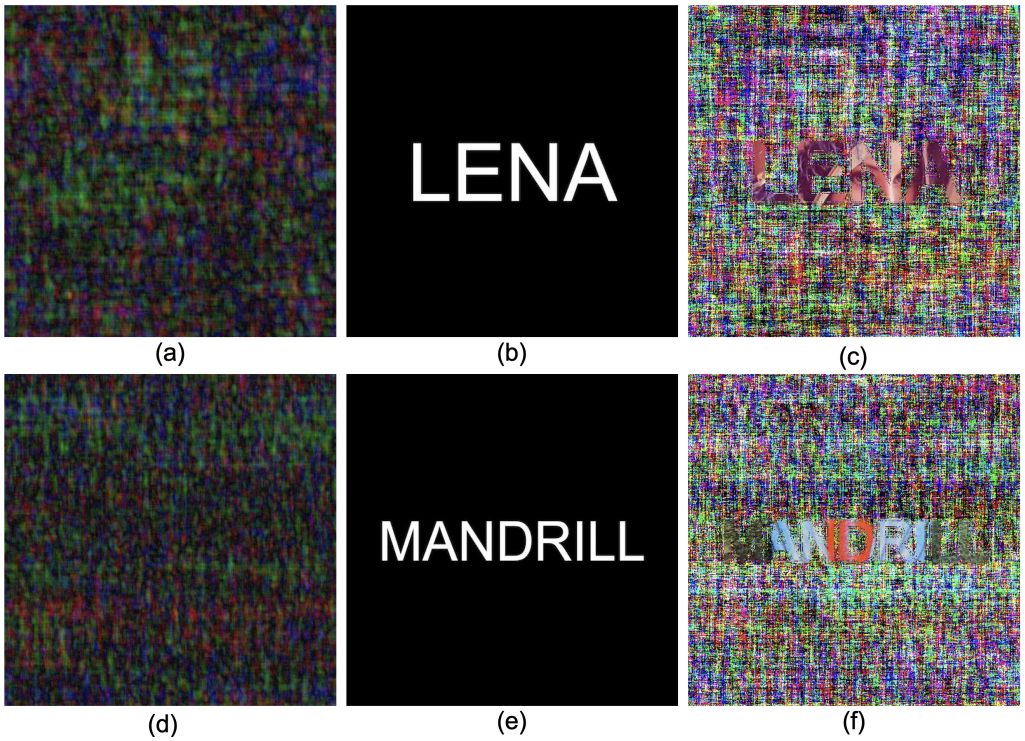


Figure 13. Decryption results by conventional DRPE for simultaneous two primary data without a constant bias ϵ: (**a**) encrypted data (**b**) primary data 1 from (**a**), (**c**) primary data 2 from (**a**), (**d**) encrypted data (**e**) primary data 1 from (**d**), and (**f**) primary data 2 from (**d**).

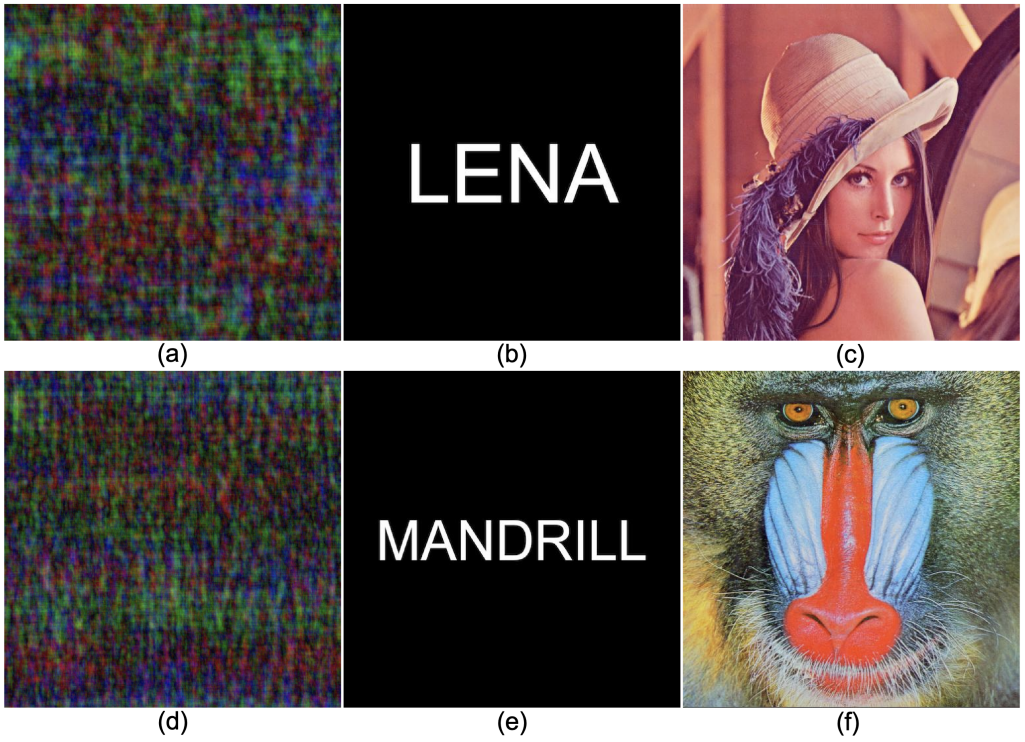


Figure 14. Decryption results by proposed DRPE for simultaneous two primary data with a constant bias of $\epsilon = 0.1$: (**a**) encrypted data (**b**) primary data 1 from (**a**), (**c**) primary data 2 from (**a**), (**d**) encrypted data (**e**) primary data 1 from (**d**), and (**f**) primary data 2 from (**d**).

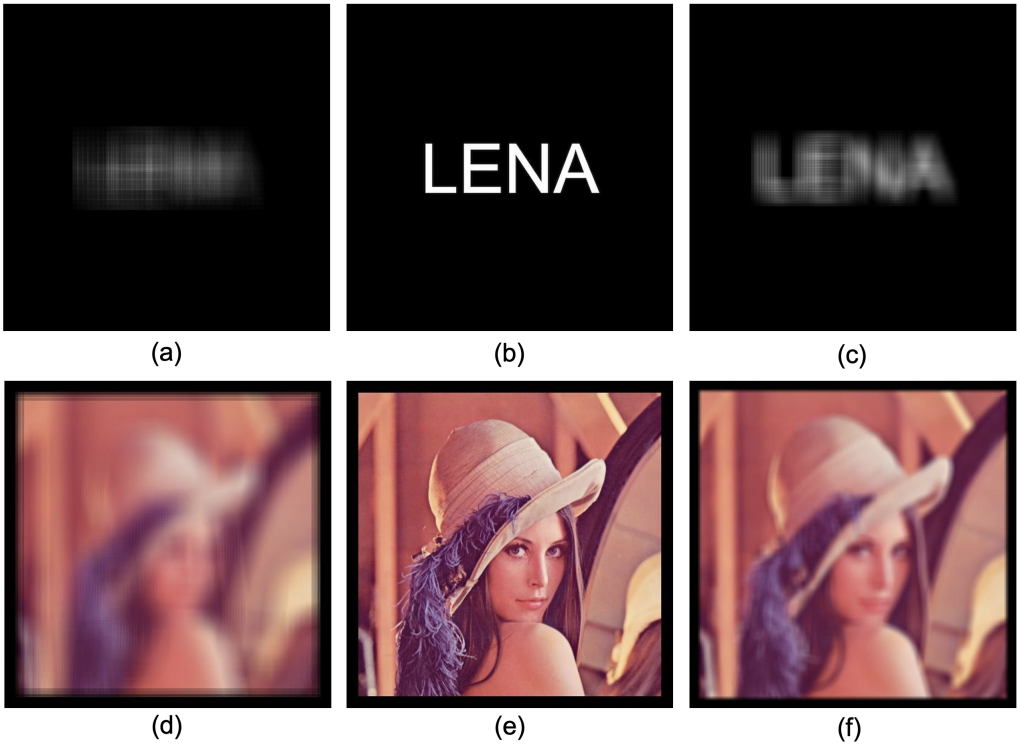


Figure 15. 3D reconstruction results for decrypted LENA text and Lena image. (**a**) z_r = 250 mm, (**b**) z_r = 512 mm, (**c**) z_r = 1000 mm, (**d**) z_r = 500 mm (**e**) z_r = 1024 mm, and (**f**) z_r = 1500 mm.

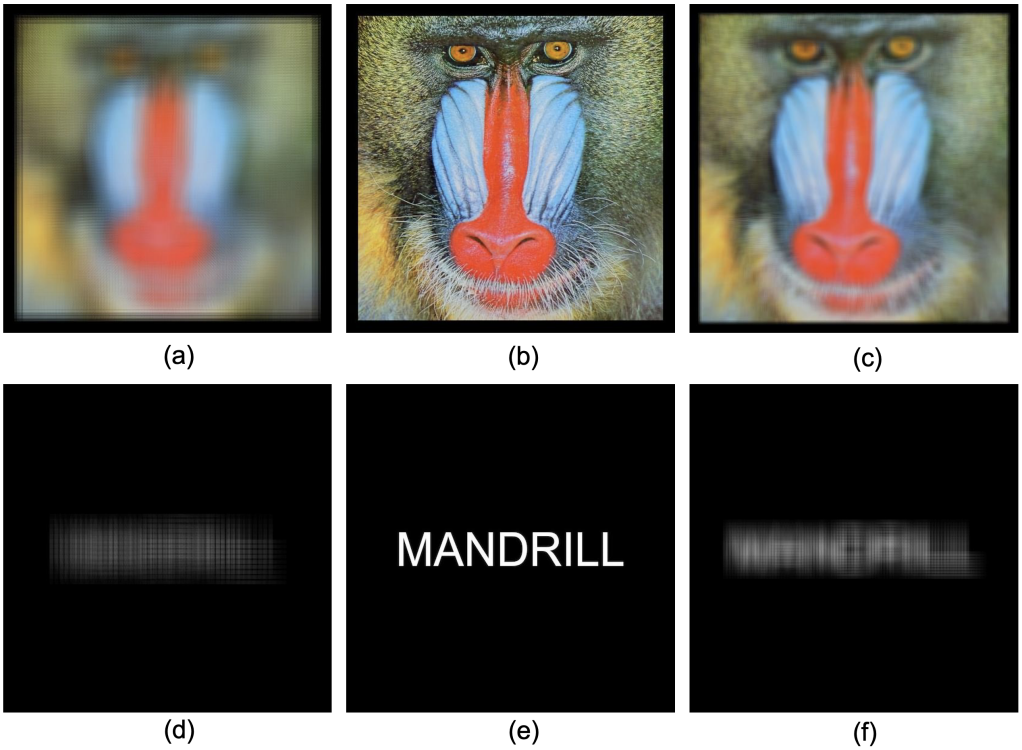


Figure 16. 3D reconstruction results for decrypted MANDRILL text and Mandrill image. (**a**) z_r = 250 mm, (**b**) z_r = 512 mm, (**c**) z_r = 1000 mm, (**d**) z_r = 500 mm (**e**) z_r = 1024 mm, and (**f**) z_r = 1500 mm.

By applying the proposed biased encoding method with a constant bias of $\epsilon = 0.1$, the phase information is preserved even in the dark regions of the first primary dataset. Furthermore, the noise previously observed in the lossy phase component is effectively eliminated. For the Lena dataset, the second primary dataset achieves a high PSNR of 59.9642 dB and an SSIM of 1. For the Mandrill dataset, the second primary dataset also exhibits a high PSNR of 49.5853 dB and an SSIM of 0.9998, as shown in Table 1. Therefore, the PSNR and SSIM of the second dataset increase significantly, resulting in a more balanced and reliable encryption system for both datasets.

Table 1. Peak signal-to-noise ratio (PSNR) and structural similarity index measure (SSIM) for 2D decrypted data by conventional DRPE for simultaneous two primary data and our method.

Method	**Conventional Method**		**Our Proposed Method**	
Metric	**PSNR [dB]**	**SSIM**	**PSNR [dB]**	**SSIM**
LENA text	57.1856	0.9995	57.1856	0.9995
Lena test	8.2346	0.0665	59.9642	1
MANDRILL text	55.8164	0.9993	55.8164	0.9993
Mandrill test	8.2869	0.0460	49.5853	0.9998

5.4. 3D Volumetric Reconstruction and Depth Security

Using volumetric computational reconstruction (VCR), we reconstructed the 3D images at different depths, as shown in Figures 15 and 16. At a depth of 512 mm, the text images "LENA" and "MANDRILL" appeared in focus, while the Lena and Mandrill test images remained blurred in the background. At 1024 mm, the Lena and Mandrill test images were clearly reconstructed, whereas the "LENA" and "MANDRILL" text data became unrecognizable.

Figure 17 shows the PSR graph across various reconstruction depths. As indicated by the PSR analysis, the peak values for the first and second datasets were located at 512 mm and 1024 mm, respectively. The sharp correlation peaks at these depths confirm that the reconstruction depth functions as a robust secondary security key. Even if the DRPE random phase mask were revealed, an unauthorized user would still require the precise longitudinal depth to recover the primary information.

5.5. Data Efficiency and Security Discussion

Data efficiency is a crucial factor for 3D systems. In this experiment, the conventional DRPE required approximately 255 MB to transmit the 9×9 elemental images for two primary datasets. Our proposed simultaneous method successfully reduced this capacity to approximately 127 MB. Furthermore, integrating the averaging operation into the VCR process helps suppress the decryption noise inherent in the phase component. By resolving the zero-amplitude singularity, we have addressed one of the three major drawbacks identified in DRPE for the simultaneous encryption of two primary datasets—the inaccuracy of phase reconstruction—thereby establishing simultaneous encryption as a viable standard for high-security 3D data transmission.

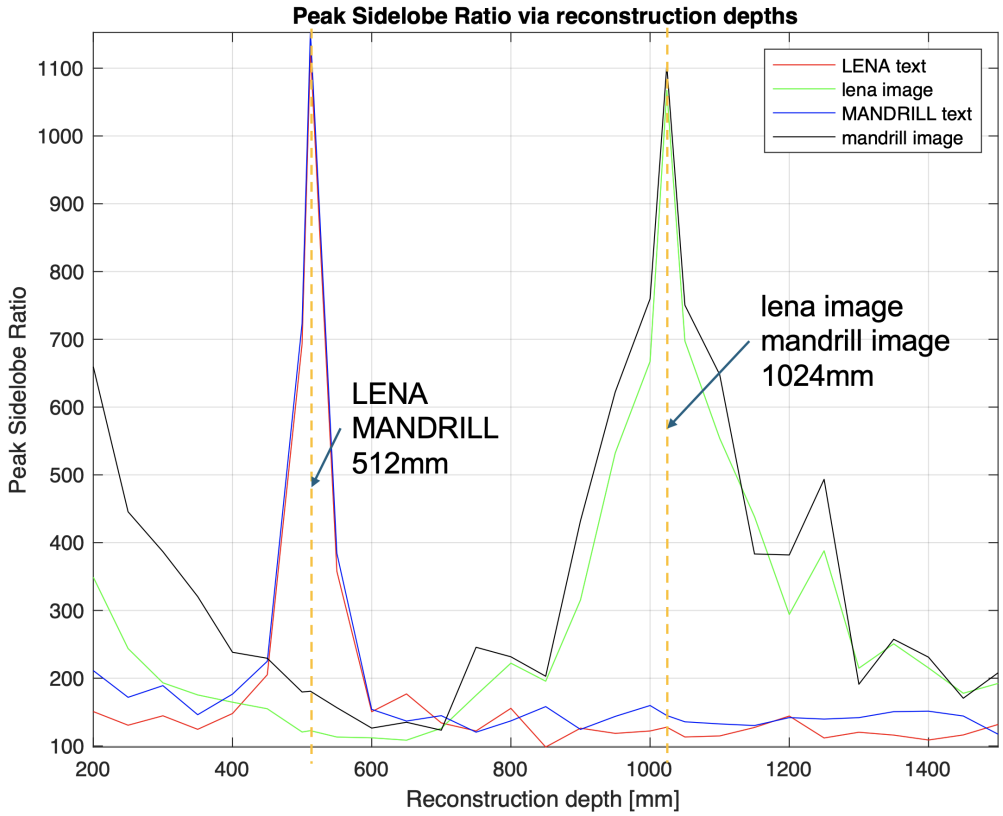


Figure 17. Peak sidelobe ratio (PSR) results for LENA text, Lena image, MANDRILL text, and Mandrill image via different reconstruction depths.

6. Conclusions

In this paper, we proposed an enhanced three-dimensional (3D) optical encryption method for the simultaneous encryption of two primary datasets using double random phase encryption (DRPE), specifically addressing the critical issue of phase information loss in regions of zero amplitude. The proposed method utilizes a single encrypted dataset to store two distinct primary datasets by assigning the first to the amplitude and the second to the phase component. This approach is integrated with synthetic aperture integral imaging (SAII) and volumetric computational reconstruction (VCR) to establish a robust 3D security framework. The primary achievement of this research is the improvement of data efficiency, a crucial factor for 3D imaging systems. By encrypting two primary datasets simultaneously into a single complex-valued dataset, we reduced the required data capacity for 9(H) $\times$ 9(V) elemental images from 255 MB to 127 MB, representing a 50% improvement over conventional DRPE methods. Furthermore, we successfully addressed the inherent drawback of simultaneous encryption, in which the phase component of the decrypted data cannot be reconstructed accurately due to its 2π-periodic nature and dependence on non-zero-amplitude values. By implementing biased amplitude encoding, we mitigated the lossy nature of the second primary dataset. While the first primary dataset (amplitude) remains essentially losssless and the second (phase) is lossy in conventional DRPE, our method enables significantly more reliable recovery even in dark regions of the amplitude image. The security of the system is further enhanced by employing two distinct key layers: the complex conjugate random phase mask and the reconstruction depth (z_r). The experimental results based on the peak sidelobe ratio (PSR) demonstrate sharp correlation peaks at 512 mm and 1024 mm, confirming that the primary datasets can only be clearly reconstructed at the correct longitudinal depths. Even if the primary encryption key is compromised, the multi-perspective nature of SAII ensures that the

data remains unrecognizable without the precise reconstruction depth. Despite these advancements, future research should aim to further enhance data capacity. Although we addressed the issue of phase reconstruction accuracy, current methods are limited to two primary datasets due to the difficulty of separating multiple phase components from a single encrypted set. Future investigations will explore alternative strategies for separating complex multi-phase information and optimizing the small constant bias, ϵ [31], potentially enabling even higher data efficiency. In conclusion, the proposed method ensures robust phase recovery across all amplitude levels and offers a reliable, efficient, and secure solution for protecting sensitive 3D information across diverse industrial applications.

Author Contributions: Conceptualization, M.C.; methodology, M.C.; investigation, M.C. and M.-C.L.; writing—original draft preparation, M.C.; writing—review and editing, M.-C.L.; visualization, M.C.; supervision, M.-C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

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

Abbreviations

The following abbreviations are used in this manuscript:

DRPE	Double Random Phase Encryption
PSNR	Peak Signal-to-Noise Ratio
PSR	Peak Sidelobe Ratio
RPM	Random Phase Mask
SAII	Synthetic Aperture Integral Imaging
VCR	Volumetric Computational Reconstruction

References

1. Javidi, B.; Horner, J.L. Optical pattern recognition for validation and security verification. *Opt. Eng.* **1994**, *33*, 1752–1756. [CrossRef]
2. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
3. Matoba, O.; Javidi, B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. *Opt. Lett.* **1999**, *24*, 762–764. [CrossRef]
4. Tan, X.; Matoba, O.; Okada-Sudo, Y.; Ide, M.; Shimura, T.; Kuroda, K. Secure optical memory system with polarization encryption. *Appl. Opt.* **2001**, *40*, 2310–2315. [CrossRef]
5. Javidi, B.; Nomura, T. Securing information by use of digital holography. *Opt. Lett.* **2000**, *25*, 28–30. [CrossRef]
6. Mogensen, P.C.; Gluckstad, J. Phase-only optical encryption. *Opt. Lett.* **2000**, *25*, 566–568. [CrossRef] [PubMed]
7. Goudail, F.; Bollaro, F.; Javidi, B.; Refregier, P. Influence of a perturbation in a double random phase encoding system. *J. Opt. Soc. Am. A* **1998**, *15*, 2629–2638. [CrossRef]
8. Matoba, O.; Nomura, T.; Perez-Cabre, E.; Millan, M.S.; Javidi, B. Optical techniques for information security. *Proc. IEEE* **2009**, *97*, 1128–1148. [CrossRef]
9. Carnicer, A.; Montes-Usategui, M.; Arcos, S.; Juvells, I. Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* **2005**, *30*, 1644–1646. [CrossRef] [PubMed]
10. Clemente, P.; Duran, V.; Torres-Company, V.; Tajahuerce, E.; Lancis, J. Optical encryption based on computational ghost imaging. *Opt. Lett.* **2010**, *35*, 2391–2393. [CrossRef] [PubMed]
11. Liao, M.; Zheng, S.; Pan, S.; Lu, D.; He, W.; Situ, G.; Peng, X. Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Elec. Adv.* **2021**, *4*, 200016. [CrossRef]
12. Tian, P.; Su, R. A novel virtual optical image encryption scheme created by combining chaotic S-Box with double random phase encoding. *Sensors* **2022**, *22*, 5325. [CrossRef]
13. Li, M.; Wang, M.; Fan, H.; Liu, Y.; Zhang, H.; Nan, H. On the security of image cryptosystems using DRPE based on scrambling and diffusion. *Opt. Quan. Elec.* **2024**, *56*, 241. [CrossRef]

14. Markman, A.; Javidi, B.; Tehranipoor, M. Photon-counting security tagging and verification using optically encoded QR codes. *IEEE. Photo. J.* **2013**, *6*, 6800609. [CrossRef]
15. Markman, A.; Javidi, B. Full-phase photon-counting double-random-phase encryption. *J. Opt. Soc. Am. A* **2014**, *31*, 394–403. [CrossRef] [PubMed]
16. Cho, M.; Javidi, B. Three-dimensional photon counting double-random-phase encryption. *Opt. Lett.* **2013**, *38*, 3198–3201. [CrossRef]
17. Lippmann, G. La Photographie Integrale. *Comp. Ren. Acad. des Sci.* **1908**, *146*, 446–451.
18. Stern, A.; Javidi, B. Three-dimensional image sensing, visualization, and processing using integral imaging. *Proc. IEEE* **2006**, *94*, 591–607. [CrossRef]
19. Levoy, M. Light fields and computational imaging. *IEEE Comput. Mag.* **2006**, *39*, 46–55. [CrossRef]
20. Martinez-Cuenca, R.; Saavedra, G.; Martinez-Corral, M.; Javidi, B. Progress in 3-D multiperspective display by integral imaging. *Proc. IEEE* **2009**, *97*, 1067–1077. [CrossRef]
21. Jang, J.-S.; Javidi, B. Improved viewing resolution of three-dimensional integral imaging by use of nonstationary micro-optics. *Opt. Lett.* **2002**, *27*, 324–326. [CrossRef]
22. Jang, J.-S.; Javidi, B. Three-dimensional synthetic aperture integral imaging. *Opt. Lett.* **2002**, *27*, 1144–1146. [CrossRef] [PubMed]
23. Jang, J.-S.; Javidi, B. Improvement of viewing angle in integral imaging by use of moving lenslet arrays with low fill factor. *Appl. Opt.* **2003**, *42*, 1996–2002. [CrossRef] [PubMed]
24. Jang, J.-S.; Javidi, B. Large depth-of-focus time-multiplexed three-dimensional integral imaging by use of lenslets with nonuniform focal lengths and aperture sizes. *Opt. Lett.* **2003**, *28*, 1924–1926. [CrossRef] [PubMed]
25. Schulein, R.; DaneshPanah, M.; Javidi, B. 3D imaging with axially distributed sensing. *Opt. Lett.* **2009**, *34*, 2012–2014. [CrossRef]
26. Cho, M.; Shin, D. 3D integral imaging display using axially recorded multiple images. *J. Opt. Soc. Korea* **2013**, *17*, 410–414. [CrossRef]
27. Hong, S.-H.; Jang, J.-S.; Javidi, B. Three-dimensional volumetric object reconstruction using computational integral imaging. *Opt. Exp.* **2004**, *12*, 483–491. [CrossRef]
28. Cho, B.; Kopycki, P.; Martinez-Corral, M.; Cho, M. Computational volumetric reconstruction of integral imaging with improved depth resolution considering continuously non-uniform shifting pixels. *Opt. Laser Eng.* **2018**, *111*, 114–121. [CrossRef]
29. Jang, J.-Y.; Cho, M. Three-dimensional double random phase encryption for simultaneous two-primary data. *Electronics* **2024**, *13*, 823. [CrossRef]
30. Javidi, B. Nonlinear joint power spectrum based optical correlation. *Appl. Opt.* **1989**, *28*, 2358–2367. [CrossRef]
31. Huang, C.; Peng, Y.; Deng, W. A dendrite net learning multi-objective artificial bee colony algorithm for UAV. *Appl. Soft Comput.* **2026**, *189*, 114449. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.