Article

Novel Multiple-Image Encryption Scheme Based on Coherent Beam Combining and Equal Modulus Decomposition

Wei Li 1, Aimin Yan 1,*, and Hongbo Zhang 2,*

1 College of Mathematics and Science, Shanghai Normal University, Shanghai 200234, China; 100045982@smail.shnu.edu.cn
2 Department of Engineering Technology, Middle Tennessee State University, Murfreesboro, TN 37132, USA
* Correspondence: yanaimin@shnu.edu.cn (A.Y.); hbzhang@mtsu.edu (H.Z.)

Abstract: In our research, we propose a novel asymmetric multiple-image encryption method using a conjugate Dammann grating (CDG), which is based on the coherent beam combining (CBC) principle. The phase generated by the Dammann grating (DG) beam splitting system is processed and added to the image to be encrypted, and then, the ciphertexts and keys are generated by equal modulus decomposition (EMD). Decryption is to combine the beams through the CDG and collect the combined images in the far field. The proposed encryption scheme is flexible and thus extendable. CDG structure parameters, such as one period length of CDG, can be used as encryption key for the increase of the complexity. The Fresnel diffraction distance can also be used as an encryption key. The power of the combined beam is stronger than that of the single beam system, which is convenient for long-distance transmission and also easy to detect. Simulation results show that the proposed method is effective and efficient for asymmetric multiple-image encryption. Sensitivity analysis of CDG alignment has also been performed showing the robustness of the system. The influence of occlusion attack and noise attack on decryption are also discussed, which proves the stability of the system.

Keywords: multiple-image encryption; asymmetric cryptosystem; conjugate Dammann grating; equal modulus decomposition

1. Introduction

Information security is significant in ensuring the integrity of the science and engineering applications [1–3]. In comparison with the digital encryption method, optical encryption is associated with more encryption parameters thus more secure [4–6]. Taking advantage of the parallel nature of light, the optical encryption system can operate in parallel, and its operation speed is much faster than that of the digital system. The early optical encryption model created by Refregier and Javidi simply consists of the 4f encryption system known having high encryption strength [7]. Due to the increase of cryptography attacks [8,9], more advanced optical encryption methods have been further developed, including fractional Fourier transform [10], gyrator transform [11], optical scanning holography [12], ghost imaging [13], phase truncation [14]. Among them, optical superposition either coherent superposition [15] or incoherent superposition [16–18] has been actively studied. Compared with incoherent superposition, coherent superposition needs more accurate alignment, which is thus able to ensure the sensitivity of the encryption system.

More specifically, Zhang proposed a simple optical image encryption scheme based on optical coherence superposition without iterative coding [19]. The encryption of this system is based on mathematical operations, and the decryption uses a beam splitter for interference. In contrast, Kim introduced a new scheme using interference-based two-dimensional binary phase mask and encrypting multiple images simultaneously [20]. Cai proposed an asymmetric coherent optical encryption system, which mainly uses equal modulus decomposition (EMD) to decompose an image into a ciphertext and a key [21]. More recently,
Chen proposed an optical image cryptosystem based on two beam coherent superposition and unequal modulus decomposition [22]. Different from the EMD approach, the method uses common vector decomposition to complete the encryption process. Among them, the amplitude term is used as ciphertext and the phase term is used as private key. The system generates four different phases and amplitudes, which improves the security of the encryption system. Sui proposed a double image encryption method based on optical interference and logistic mapping [23]. These parameters, such as wavelength, wheelbase, and logistic mapping conditions are used as additional keys to improve the security of the system. Luan proposed an asymmetric scheme for silhouette-free multiple encryption using coherent superposition and the Fresnel transform [24]. Within this approach, the ciphertext and private key in the encryption process are obtained by random mask, and a function is constructed in the encryption process to improve the security. In addition, different images are decrypted using different private keys. Even if one or two of the correct phase masks are obtained, the information of any original image, including its contour, cannot be obtained. Abuturab proposed a multiple image encryption using Fresnel domain high-dimension chaotic phase coding [25]. In this photoelectric method, the color image is decomposed into R, G and B channels, each channel is individually phase-coded and modulated, and Fresnel transform is performed to generate the corresponding encrypted channel. It is therefore convenient to update, manage and transmit the decryption key. While these methods have proposed more secure encryption, the efficient use of beam power has not been well addressed. The applied beam is often weak thus adversely impacts the detection accuracy of an object through the decryption process, thus limiting its practical use.

In our research, a novel method for multiple-image encryption based on coherent beam combining (CBC) using a conjugate Dammann grating (CDG) is proposed. The novel method combines different numbers of beams by using different CDG, such as 3 × 3 CDG, 4 × 4 CDG, and 5 × 5 CDG, which solves the problem of weak beam energy mentioned above. Moreover, the coherent array beam parameter of CDG and Fresnel diffraction distance can also be used as the encryption key. In this scheme, eight QR codes are superimposed by bit plane, and each QR code stores an image. Random scrambling is carried out to hide the outline of the superimposed QR code. Then, the scrambled image is randomly divided into four pieces, each of which is multiplied by the corresponding Dammann phase (DP) complex conjugate. Finally, they are decomposed into ciphertexts and keys by EMD in turn. Compared with the other optical encryption system, our optical system has the following advantages. First, the one-period length of CDG can be used as one of the keys for encryption. Second, the coherent superposition is more superior to the incoherent superposition, introducing more encryption keys, such as Fresnel diffraction distance, thus more capable of resisting cryptosystem attacks. Third, the power of the combined beam is higher than the conventional methods, which is thus easy to detect. Fourth, the QR codes can ensure that the encrypted images are able to be decrypted without image quality loss. The organization of our paper is given as follows. In Section 2, theories involved in the research are introduced and described. The simulation results of our encryption system are given in Section 3. Relevant discussions are carried out in Section 4, followed by a conclusion of the research in Section 5.

2. Methods

2.1. Coherent Beam Combining

Dammann grating (DG) is a binary phase grating which can produce an equal space and intensity beam point array [26,27]. The transmission function of a DG is

\[ T_{DG}(x, y) = \exp \left[ j \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} \Delta \phi(x - mT_x, y - nT_y) \right] \]  

where \( T_x \) and \( T_y \) are the periods of DG in \( x \) and \( y \) directions, respectively, \( \Delta \phi(x, y) \) is the phase of DG in one period. When a Gaussian beam \( E(x, y) \) illuminates the DG, a Gaussian
laser array with same intensity can be generated. The electric field $E(x, y)$ of the Gaussian beam is given as

$$E(x, y) = \exp \left( -\frac{x^2 + y^2}{\omega_0^2} \right)$$  \hspace{1cm} (2)$$

where $\omega_0$ is the waist radius. The optical field at the back focal plane of the lens $L$ in Figure 1a can be expressed as

$$U(f_x, f_y) = \widetilde{E}(f_x, f_y) \otimes \widetilde{T}_{DG}(f_x, f_y)$$  \hspace{1cm} (3)$$

where $\widetilde{E}(f_x, f_y)$ and $\widetilde{T}_{DG}(f_x, f_y)$ are the Fourier transformation of $E(x, y)$ and $T_{DG}(x, y)$, respectively, and the symbol $\otimes$ represents convolution. Suppose the DG can generate $M \times N$ equally bright diffraction orders and other high orders $H(f_x, f_y)$ with little energy,

$$\widetilde{T}_{DG}(f_x, f_y) = \sum_{m} \sum_{n} \delta(f_x - \frac{m}{T_x}, f_y - \frac{n}{T_y}) C_{mn} e^{j\phi_{mn}} + H(f_x, f_y),$$  \hspace{1cm} (4)$$

where $\delta(x, y)$ is Dirac function, $C_{mn}$ and $\phi_{mn}$ (DP) are the amplitude and phase of the diffraction order $(m, n)$. By optimizing the parameters of the DG, $H(f_x, f_y)$ can be very small or even close to 0, that is, the diffraction efficiency is close to 100%. Then, Equation (3) can be simplified as

$$U(f_x, f_y) = \sum_{m} \sum_{n} \widetilde{E}(f_x - \frac{m}{T_x}, f_y - \frac{n}{T_y}) C_{mn} e^{j\phi_{mn}}$$  \hspace{1cm} (5)$$

When using CDG to combine the beam as shown in Figure 1b, we assume that the array beam is a perfect coherent laser. At the same time, the phase plate (PP) used in the beam combining system is the complex conjugate of the phase $\phi_{mn}$ in Equation (4), expressed by $\phi_{mn}^*$. The phase distribution of the CDG is the complex conjugate of the DG, expressed by $T_{DG}^*(x, y)$. The laser array field distribution after the PP in Figure 1b is

$$E_1(f_x, f_y) = e_s(f_x, f_y) \otimes \sum_{m} \sum_{n} \delta(f_x - \frac{m}{T_x}) \delta(f_y - \frac{n}{T_y}) e^{j\phi_{mn}^*}.$$  \hspace{1cm} (6)$$

where $e_s(f_x, f_y)$ is a function of the incident laser. Because the relationship between the front focal plane and the back focal plane of the lens can be transformed into Fourier transform calculation, we simplify the optical field at the back focal plane of the lens $L$ in Figure 1b as $\widetilde{E}_1(x, y) \propto \mathcal{F}\{E_1(f_x, f_y)\}$, where $\mathcal{F}$ is the Fourier transformation. By combining Equations (5) and (6), $\widetilde{E}_1(x, y)$ can be rewritten as

$$\widetilde{E}_1(x, y) \propto \mathcal{F}\{e_s(f_x, f_y)\} \frac{T_{DG}^*(-x, -y)}{C_{mn}}.$$  \hspace{1cm} (7)$$

Therefore, the expression of optical field behind the CDG is

$$E_2(x, y) = \widetilde{E}_1(x, y) T_{DG}^*(-x, -y) \propto \mathcal{F}\{e_s(f_x, f_y)\}.$$  \hspace{1cm} (8)$$

From the results of Equation (8), it can be seen that the CDG can effectively eliminate the phase change during beam combination, so as to obtain a uniform optical field distribution, and a better single beam spot can be obtained in the far-field observation. In our work, we can generate $2 \times 2$ array beam by specially designing the structure of DG. The simulation of generating array beams is shown in Figure 2a,b. The simulation of the $2 \times 2$ CDG used for beam combining is shown in Figure 2c–e. In addition, the simulation shows that the square array beam can also be used for beam combination, and the final beam
combination spot is still square, which provides convenience for our subsequent image encryption.

Figure 1. (a,b) The beam splitting system diagram and beam combining system diagram of $2 \times 2$ DG, respectively. DG, Dammann grating; L, Fourier lens; PP, phase plate; CDG, conjugate Dammann grating.

Figure 2. (a,b) Simulation diagram of the intensity and phase of the rear focal plane of the lens L in beam splitting respectively; (c,d) simulation diagram of the intensity and phase of the front focal plane of the lens L in beam combining, respectively; (e) the beam intensity distribution map of the far field in beam combining.

Next, we will introduce the theory of equal modulus decomposition (EMD) [21] in detail. Generally speaking, a complex number can be expressed as a position vector in the two-dimensional Cartesian coordinate system space. It consists of a horizontal real part (Re) component and a vertical imaginary part (Im) component, as shown in Figure 3. According to this, the EMD is produced through an asymmetric mathematical transformation. Here, we use the simplest one-dimensional symbol to describe the process. Assume that the intensity of the original image is $O(x)$ and the phase added to the image is $P$, the new function is constructed as follows

$$I(x) = \sqrt{O(x)} \cdot P$$  \(9\)

In addition, $I(x)$ can be divided into two complex numbers $M_1(x)$ and $M_2(x)$ with equal modulus, as shown in Figure 3. The expression of $\theta(x)$ is

$$\theta(x) = 2\pi rand(x),$$  \(10\)
where \( \text{rand}(x) \) is a function that can generate random numbers in the range of \([0, 1]\). Moreover, the expressions of \( M_1(x) \) and \( M_2(x) \) are

\[
M_1(x) = \frac{A(x)/2}{\cos[\varphi(x) - \theta(x)]} \exp[i\theta(x)], \quad (11)
\]

\[
M_2(x) = \frac{A(x)/2}{\cos[\varphi(x) - \theta(x)]} \exp\{i[2\varphi(x) - \theta(x)]\}, \quad (12)
\]

where \( A(x) = |I(x)| \) and \( \varphi(x) = \arg\{I(x)\} \). Finally, an image information \( I(x) \) is successfully hidden into two complex numbers \( M_1(x) \) and \( M_2(x) \) by using the EMD principle. In this process, \( I(x) \) can only be obtained from \( M_1(x) \) when \( M_2(x) \) is known. Therefore, \( M_2(x) \) can be regarded as the private key. \( M_1(x) \) is the ciphertext, and \( \theta(x) \) is the public key for image encryption.

![Figure 3](image-url)  
**Figure 3.** The schematic diagram of EMD for illustration of the relationship between \( I(x) \), \( M_1(x) \), and \( M_2(x) \).

### 2.2. Cryptosystem

Based on the above principles, we will describe the pure digital encryption process as shown in Figure 4a in detail. Firstly, eight QR codes \( Q_i, i = 1, 2, 3, 4, 5, 6, 7, 8 \) which record eight images are superimposed in bit plane mode as shown in Equation (13) to obtain a superimposed image \( Q \). Secondly, the superimposed image \( Q \) is randomly scrambled by pixels into image \( D \), and then randomly divided into four images \( D_1, D_2, D_3, \) and \( D_4 \) similar to random decomposition of numbers (e.g., \( 255 = 80 + 66 + 57 + 52 \)). Thirdly, each image \( D_1, D_2, D_3, \) and \( D_4 \) is multiplied by the phase of the PP \( P_1, P_2, P_3, P_4 \) in Figure 2d to obtain four complex values. Finally, according to EMD principle, each complex value is decomposed into two parts, one part is four ciphertexts \( C_1, C_2, C_3, \) and \( C_4 \), and the other part is four keys \( K_1, K_2, K_3, \) and \( K_4 \).

In the process of decryption, as shown in Figure 4b, first, the added ciphertexts and keys are loaded on the front focal plane of the lens \( L \) in Figure 4b by SLM, and it can be considered to load the ciphertexts and keys, respectively, with the help of 4f imaging system. Second, the square root of the intensity distribution obtained in the far field is normalized to \([0, 255]\), which is image \( D \). Third, the normalized image \( D \) is inversely scrambled to obtain image \( Q \), and the \( Q \) is decomposed into eight QR codes in bit plane mode as shown in Equation (14). Finally, the corresponding original image can be obtained by scanning each QR code.

\[
Q = 2^0Q_1 + 2^1Q_2 + 2^2Q_3 + 2^3Q_4 + 2^4Q_5 + 2^5Q_6 + 2^6Q_7 + 2^7Q_8, \quad (13)
\]
where \( \text{floor} \) is rounded down to the closest integer.

\[
\begin{align*}
Q_8 &= \text{floor}(Q/2^7), \\
Q_7 &= \text{floor}\left[\frac{Q - 2^7Q_8}{2^6}\right], \\
Q_6 &= \text{floor}\left[\frac{Q - 2^7Q_8 - 2^6Q_7}{2^5}\right], \\
Q_5 &= \text{floor}\left[\frac{Q - 2^7Q_8 - 2^6Q_7 - 2^5Q_6}{2^4}\right], \\
Q_4 &= \text{floor}\left[\frac{Q - 2^7Q_8 - 2^6Q_7 - 2^5Q_6 - 2^4Q_5}{2^3}\right], \\
Q_3 &= \text{floor}\left[\frac{Q - 2^7Q_8 - 2^6Q_7 - 2^5Q_6 - 2^4Q_5 - 2^3Q_4}{2^2}\right], \\
Q_2 &= \text{floor}\left[\frac{Q - 2^7Q_8 - 2^6Q_7 - 2^5Q_6 - 2^4Q_5 - 2^3Q_4 - 2^2Q_3}{2^1}\right], \\
Q_1 &= \text{floor}\left[\frac{Q - 2^7Q_8 - 2^6Q_7 - 2^5Q_6 - 2^4Q_5 - 2^3Q_4 - 2^2Q_3 - 2^1Q_2}{2^0}\right]
\end{align*}
\]

3. Simulation

We have conducted simulations to demonstrate the feasibility and effectiveness of the proposed method. The pixel size of the original eight gray images is \(256 \times 256\), and the pixel size of the eight QR codes thus converted is \(58 \times 58\), in which the original images are selected from the public encrypted image set commonly used in the field of image encryption. The simulation diagram of encryption process is shown in Figure 5, and the simulation diagram of decryption process is shown in Figure 6. By using a QR code scanner to scan the decrypted eight QR codes, eight original images can be obtained. The errors and attacks of these simulation results will be discussed in the next section.
Figure 5. (a,b) Superimposed image Q and scrambled image D; (c–f) four divided images $D_1$, $D_2$, $D_3$ and $D_4$; (g–j) four ciphertexts $C_1$, $C_2$, $C_3$ and $C_4$; (k–n) four keys $K_1$, $K_2$, $K_3$ and $K_4$.

Figure 6. (a) Decrypted superimposed image Q; (b–i) eight decrypted QR codes.
4. Discussion

4.1. Error Analysis

Structure similarity (SSIM) is used for evaluating the effect of encryption system. The equation of SSIM is shown as follows

\[
\text{SSIM} = \left( \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \right) \left( \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \right) \left( \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \right)
\]

where \(\mu_x\) and \(\mu_y\) are the mean of the original image and the decrypted image, respectively, \(\sigma_x\) and \(\sigma_y\) are the variance of the original image and the decrypted image, respectively, \(\sigma_{xy}\) is the covariance between the original image and the decrypted image, \(C_1, C_2, C_3\) are small constants. According to Equation (7), when the array beam loaded with the images is transformed by the Fourier lens, the phase distribution is consistent with the amplitude transmittance function of the CDG on the focal plane behind the Fourier transform lens, and the beam field distribution can be regarded as a virtual grating. By multiplying the matched CDG, the two-phase cancellation can obtain the beam field with uniform distribution. However, because the phase distribution of the beam field on the back focal plane is not visible, the virtual grating and the CDG must be aligned strictly in order to effectively eliminate the phase fluctuation of the combined beam field. Therefore, it is necessary to calculate the encryption effect when the CDG is translated along the grating period direction. Figure 7a shows the SSIM between the decrypted image and the original image when the CDG is shifted \(x\) cycles along the horizontal direction. At the same time, the phase value of the PP will also affect the decryption effect. For this, we add random phase errors in the range of 0 to \(\pi\) for the PP value in the simulation, where \(0 < \alpha < 0.5\). Figure 7b shows the SSIM between the decrypted image and the original image when the PP value is associated with errors. As shown in Figure 7b, with the increase of the PP value error, the quality of decrypted image becomes worse. It shows that when the PP value error is small, the lossless image decryption can be achieved.

![SSIM graphs](image)

Figure 7. (a) The SSIM between the decrypted image and the original image when the CDG moves horizontally for \(x\) cycles; (b) the SSIM between the decrypted image and the original image when the PP value is associated with errors in the range of 0 to \(\pi\).

4.2. Occlusion Attack Analysis

Generally speaking, hackers may attack the ciphertexts and cause partial loss of the ciphertexts [28]. Therefore, it is necessary to discuss the influence of the lost part of ciphertexts on the decryption in the process of transmission. At present, we have four ciphertexts. If we cut them by 5%, 10% and 15%, respectively, four ciphertexts and eight decrypted QR codes are shown in Figure 8. As can be seen from the figure, the original image can still be obtained, so our encryption system can well resist occlusion attack.
Figure 8. Cont.
4.3. Noise Attack Analysis

In addition, a common noise attack in the field of image encryption needs to be discussed. Because there is noise in the process of ciphertexts transmission or hackers deliberately add noise to the ciphertexts to disturb the decrypted results, we add salt and pepper noise to the ciphertexts to test the anti-noise ability of the system. After adding salt and pepper noises with densities of 0.05, 0.1, and 0.2 to the four ciphertexts (which are proportional to the total number of pixels of the noise points), Figure 9 shows the four ciphertext images and the associated reconstructed images under different noise densities. The results show that even if significant salt and pepper noise is introduced, the original images can still be reconstructed from the decrypted QR codes, which shows that our system can effectively resist noise attacks.

4.4. Key Space and Exhaustive Search Attack Analysis

The proposed encryption scheme has high strength for resisting the exhaustive search attack. In this scheme, the secret key (58 by 58 matrix, each element with value of complex number) space of the encryption system is greater than $2^{100}$, therefore will take significant computational power for exhaustive search able to attack the proposed scheme. More specifically, the secret key is a complex matrix generated by EMD. In our research, the size of matrix is $58 \times 58$, which also can be expanded depending on the need. Furthermore, the value of the matrix is a complex number, which further increases the complexity for resisting the exhaustive search attack.

4.5. Known Plaintext Attack Analysis

In addition to the exhaustive search attack, a known plaintext attack is also a common attack type [29]. The purpose of this attack is to obtain the decryption secret key through the attack, so as to crack other ciphertexts. However, this attack is invalid for our system, because our decryption secret key depends on the original image. If the original image is different, the secret key will be different. In other words, even if the attacker obtains the secret key of the known plaintext through some means, the attacker can only decipher the current plaintext and cannot decipher other plaintext. Therefore, our proposed scheme is immune to this attack scheme.

4.6. Noise Cross-Talk Analysis

It is known that the conventional multiple-image encryption is vulnerable to noise cross-talk. In contrast to conventional image encryption, in the proposed scheme, multiple
binary QR codes are mathematically superimposed with different coefficients during encryption. Because different coefficients are independent of each other, it ensures that each image is independent of each other without image noise cross-talk. In the image decryption phase, each image is separated through the inverse image scrambling process therefore to ensure that there is no noise cross-talk either. As such, the image cross-talk noise problem is avoided.

Figure 8.

(a1)–(d1) 5% occlusion ciphertext images; (e1)–(l1) decrypted images corresponding to (a1)–(d1); (a2)–(d2) 10% occlusion ciphertext images; (e2)–(l2) decrypted images corresponding to (a2), (d2); (a3)–(d3) 15% occlusion ciphertext images; (e3)–(l3) decrypted images corresponding to (a3), (d3).

4.3. Noise Attack Analysis

In addition, a common noise attack in the field of image encryption needs to be discussed. Because there is noise in the process of ciphertexts transmission or hackers deliberately add noise to the ciphertexts to disturb the decrypted results, we add salt and pepper noise to the ciphertexts to test the anti-noise ability of the system. After adding salt and pepper noises with densities of 0.05, 0.1, and 0.2 to the four ciphertexts (which are proportional to the total number of pixels of the noise points), Figure 9 shows the four ciphertext images and the associated reconstructed images under different noise densities. The results show that even if significant salt and pepper noise is introduced, the original images can still be reconstructed from the decrypted QR codes, which shows that our system is robust to noise attacks.

Figure 9. Cont.
Figure 9. (a1–d1) Ciphertext images after adding salt and pepper noise of 0.05 density; (e1–l1) decrypted images corresponding to (a1–d1); (a2–d2) ciphertext images after adding salt and pepper noise of 0.1 density; (e2–l2) decrypted images corresponding to (a2–d2); (a3–d3) ciphertext images after adding salt and pepper noise of 0.2 density; (e3–l3) decrypted images corresponding to (a3–d3).
4.7. Main Advantages

It is worth noting that coherent superposition has been used by some previous methods [15,22,24], but these superposition methods have not used multiple light beams as used in this study, thus suffering low energy efficiency usages. Our method, in principle, can synthesize at least four beams simultaneously, furthermore, nine beams, sixteen beams, twenty-five beams are also feasible, especially with the VCSEL & SPAD technology, where multiple lasers can be made possible in a small footprint place. The laser combination technique used in this study greatly improved the power of optical decryption images and, thus, significantly improved the image reconstruction quality, especially for remote sensing applications. With regard to RGB image encryption, different from the previous method, where typically an image is decomposed to three-color channels and then encrypting them respectively [25]. In contrast to previous approach, in this study, the color image is converted to QR code before encryption and converted back to color image using QR code following decryption therefore to address the color image encryption problem with minimum amount of hardware investment. In terms of encryption and decryption time, the scheme is a hybrid optoelectronic system; thus, it can take advantages of utilizing existing digital encryption methods [30–33] but also optical encryption schemes as well [10–14]. Time efficient multiplication and addition are used in the digital encryption process. Meanwhile, the operation of optical encryption is a parallel operation process. Therefore, the encryption speed is more efficient than the pure digital image encryption schemes such as chaotic encryption and elliptic curve cryptography [18].

5. Conclusions

In conclusion, we have proposed a novel method for multiple-image encryption based on coherent beam combing using conjugate Dammann grating. In our research, our method has illustrated the coherent array beam combination working principle for achieving multiple-image encryption. The proposed system has the following advantages. First, our simulation uses $2 \times 2$ CDG, but it can be extended to higher order of CDG, such as $3 \times 3$ CDG and $5 \times 5$ CDG, or even higher-order CDG, as such multiple images can be encrypted at the same time. Second, other parameters of CDG can also be used as encryption parameters. For example, the structure of CDG, such as the length of a single period, can also be used as a key to provide higher security for the encryption system. Finally, due to the combination effect of CDG, the signal strength of beam after the array images is strong and thus easy to detect, which is the biggest advantage of our encryption system. In addition, we discuss the influence of CDG alignment and PP value errors on encryption. We also discuss the influence of occlusion attack and noise attack on decryption. Our research demonstrates a new scheme for high-power multiple image encryption, which can find rich engineering applications.

Author Contributions: Conceptualization and methodology, A.Y. and W.L.; writing—original draft preparation, W.L.; reviewing and editing, H.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Nature Science Foundation of China under grant no. 62075134.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

1. Matoba, O.; Nomura, T.; Perez-Cabre, E.; Millan, M.; Javidi, B. Optical techniques for information security. *Proc. IEEE*. 2009, 97, 1128–1148. [CrossRef]

2. Manzo, M. KGearsRG: Kernel Graph Embedding on Attributed Relational SIFT-Based Regions Graph. *Mach. Learn. Knowl. Extr.* 2019, 1, 962–973. [CrossRef]

3. Flores-Vergara, A.; Inzunza-González, E.; García-Guerrero, E.E.; López-Bonilla, O.R.; Rodríguez-Orozco, E.; Hernández-Ontiveros, J.M.; Cárdenas-Valdez, J.R.; Tlelo-Cuautle, E. Implementing a Chaotic Cryptosystem by Performing Parallel Computing on Embedded Systems with Multiprocessors. *Entropy* 2019, 21, 268. [CrossRef]

4. Ghadirli, H.; Nodehi, A.; Enayatifar, R. An overview of encryption algorithms in color images. *Signal. Process.* 2019, 164, 163–185. [CrossRef]

5. Kaur, M.; Kumar, V. A comprehensive review on image encryption techniques. *Arch. Comput. Methodol. E.* 2020, 27, 15–43. [CrossRef]

6. Chen, W.; Javidi, B.; Chen, X. Advances in optical security systems. *Adv. Opt. Photonics*. 2014, 6, 120–155. [CrossRef]

7. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* 1995, 20, 767–769. [CrossRef] [PubMed]

8. Chen, L.; Peng, B.; Gan, W.; Liu, Y. Plaintext attack on joint transform correlation encryption system by convolutional neural network. *Opt. Exp.* 2020, 28, 28154–28163. [CrossRef]

9. Chang, X.; Yan, A.; Zhang, H. Ciphertext-only attack on optical scanning cryptography. *Opt. Laser. Eng.* 2020, 126, 105901. [CrossRef]

10. Wang, X.; Su, Y. Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform. *Sci. Rep.* 2020, 10, 18556. [CrossRef]

11. Yan, A.; Dong, J.; Li, Y. A novel nonlinear double image encryption based on affine transform and gyror transform. *J. Opt.* 2018, 20, 115702. [CrossRef]

12. Yan, A.; Wei, Y.; Zhang, J. Security enhancement of optical encryption based on biometric array keys. *Opt. Commun.* 2018, 419, 134–140. [CrossRef]

13. Zhang, L.; Zhang, Z.; Kang, Y.; Ye, H.; Xiong, R.; Yuan, X.; Wang, Z.; Wang, K.; Zhang, D. Research on double-layers optical information encryption based on ghost imaging. *Opt. Commun.* 2020, 455, 124585. [CrossRef]

14. Qin, W.; Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* 2010, 35, 118–120. [CrossRef]

15. Zhong, Z.; Qin, H.; Liu, L.; Zhang, Y.; Shan, M. Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain. *Opt. Exp.* 2017, 25, 6974–6982. [CrossRef]

16. Chen, L.; Chang, G.; He, B.; Mao, H.; Zhao, D. Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition. *Opt. Laser. Eng.* 2017, 88, 221–232. [CrossRef]

17. Shi, Y.; Liu, Y.; Sheng, W.; Zhu, D.; Wang, J.; Wu, T. Multiple-image double-encryption via 2D rotations of a random phase mask with spatially incoherent illumination. *Opt. Exp.* 2019, 27, 26050–26059. [CrossRef]

18. Li, W.; Chang, X.; Yan, A.; Zhang, H. Asymmetric multiple image elliptic curve cryptography. *Opt. Laser. Eng.* 2021, 136, 106319. [CrossRef]

19. Zhang, Y.; Wang, B. Optical image encryption based on interference. *Opt. Lett.* 2008, 33, 2443–2445. [CrossRef] [PubMed]

20. Kim, Y.; Song, J.; Moon, I.; Lee, Y. Interference-based multiple-image encryption using binary phase masks. *Opt. Laser. Eng.* 2018, 107, 281–287. [CrossRef]

21. 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]

22. Chen, L.; Gao, X.; Chen, X.; He, B.; Liu, J.; Li, D. A new optical image cryptosystem based on two-beam coherent superposition and unequal modulus decomposition. *Opt. Laser Technol.* 2016, 78, 167–174. [CrossRef]

23. Sui, L.; Du, C.; Zhang, X.; Tian, A.; Anand, A. Double-image encryption based on interference and logistic map under the framework of double random phase encoding. *Opt. Laser. Eng.* 2019, 122, 113–122. [CrossRef]

24. Luan, G.; Chen, Z.; Huang, C. Silhouette-free multiple image encryption using coherent superposition and Fresnel transform. *Optik* 2020, 224, 165498. [CrossRef]

25. Abuturab, M.R. A superposition based multiple-image encryption using Fresnel-Domain high dimension chaotic phase encoding. *Opt. Lasers Eng.* 2020, 129, 106038. [CrossRef]

26. Zhou, C.; Liu, L. Numerical study of Dammann array illuminators. *Appl. Opt.* 1995, 34, 5961–5969. [CrossRef] [PubMed]

27. Li, S.; Lu, Y. Coherent beam combination using non-separable phase-controlled Dammann grating. *Opt. Commun.* 2018, 407, 321–326. [CrossRef]

28. Murillo-Escobar, M.; Meranza-Castillon, M.; Lopez-Gutierrez, R.; Cruz-Hernandez, C. Suggested Integral Analysis for Chaos-Based Image Cryptosystems. *Entropy* 2019, 21, 815. [CrossRef]

29. Alvarez, G. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcation. Chaos*. 2006, 16, 2129–2151. [CrossRef]

30. Flores-Vergara, A.; García-Guerrero, E.; Inzunza-González, E.; López-Bonilla, O.; Rodríguez-Orozco, E.; Cardenas-Valdez, J.; Tlelo-Cuautle, E. Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. *Nonlinear. Dyn.* 2019, 96, 497–516. [CrossRef]
31. De la Fraga, L.G.; Mancillas-Lopez, C.; Tlelo-Cuautle, E. Designing an authenticated Hash function with a 2D chaotic map. *Nonlinear Dyn.* **2021**, *104*, 4569–4580. [CrossRef]

32. González-Zapata, A.M.; Tlelo-Cuautle, E.; Cruz-Vega, I.; Leon-Salas, W.D. Synchronization of chaotic artificial neurons and its application to secure image transmission under MQTT for IoT protocol. *Nonlinear Dyn.* **2021**, *104*, 4581–4600. [CrossRef]

33. Liang, H.; Zhang, G.; Hou, W.; Huang, P.; Liu, B.; Li, S. A Novel Asymmetric Hyperchaotic Image Encryption Scheme Based on Elliptic Curve Cryptography. *Appl. Sci.* **2021**, *11*, 5691. [CrossRef]