Article

A Multi-Image Encryption with Super-Lager-Capacity Based on Spherical Diffraction and Filtering Diffusion

Hanmeng Wu, Jun Wang , Ziyi Zhang, Xudong Chen and Zheng Zhu

School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China; hanmeng_wu@163.com (H.W.); ziyi1040363061@163.com (Z.Z.); helloxudong@outlook.com (X.C.); zzhu0420@163.com (Z.Z.)

* Correspondence: jwang@scu.edu.cn

Received: 18 July 2020; Accepted: 14 August 2020; Published: 17 August 2020

Abstract: A multi-image encryption with super-large-capacity is proposed by using spherical diffraction and filtering diffusion. In the proposed method, initial images are processed sequentially by filtering diffusion and chaos scrambling. The images are combined into one image using XOR operation. The combined image is encrypted by improved equal modulus decomposition after spherical diffraction. There are three main contributions of the proposed method—(1) resisting phase-retrieval attack due to the asymmetry of spherical diffraction; (2) high flexibility of decrypting images individually; and (3) super-large encryption capacity of the product of image resolution and grayscale level, which is the most significant advantage. The feasibility and effectiveness of the proposed encryption are verified by numerical simulation results.

Keywords: multi-image encryption; spherical diffraction; filtering diffusion

1. Introduction

With the development of information technology, how to ensure the security of image information becomes an essential point. In image encryption research, optical information processing technology and digital technology have been widely used in image encryption [1–7]. Refregier and Javidi proposed double random phase encoding (DRPE) in 1995, which pioneered the field of optical encryption [8]. However, because of the linear symmetry of DRPE technology [9], it is proved to be vulnerable to the known-plaintext attack [10] and chosen-plaintext attack [11]. To improve security, several nonlinear cryptosystems are proposed to improve the weaknesses of traditional symmetric cryptosystems, such as Fresnel domain [12], cylindrical diffraction transform [13–15], gyrator transform domain [16], and fractional Mellin transform [17]. However, these image encryption methods are usually applied to encrypt one image, which has made it challenging to meet the growing information needs. Recently, more and more scholars have begun to study multi-image encryption [18–23].

Multi-image encryption can be divided into two categories according to the encryption process. One of the multi-image encryption technologies is based on cascading [24–26]. Sui et al. [27] used cascaded fractional Fourier transform to encrypt multiple images. As the number of images increases, the quality of decryption decreases rapidly. Li et al. [28] proposed a multiple-image encryption method using the cascaded fractional Fourier transform, which cannot get a decrypted image individually from the ciphertext. Hence, the decryption flexibility is poor, and the number of encryption images is severely limited. The other multi-image encryption technology is based on multiplexing, such as space multiplexing [29], region multiplexing [30], wavelength multiplexing [31,32], and position multiplexing [33]. For instance, Deepan et al. [34] proposed a multi-image cryptosystem based on compressive sensing and the DPPE technique. By this method, the space multiplexing method is also used to integrate multiple-image data. Zhao et al. [35] came up with a multi-image encryption

by using the position multiplexing. Besides, Hu et al. [36] proposed an asymmetric multi-image encryption using the convolution multiplexing. Due to crosstalk issues, this method can only encrypt up to 12 images. Moreover, Liu et al. [37] present a double image encryption using fractional order multiplexing to combine two initial images. Because of the characteristics of multiplexing technology, it can decrypt images individually, which has high decryption flexibility. In the process of information multiplexing, the information of different images occupies the same channel. However, the traditional multiplexing method will lead to data crosstalk and the limited encryption capacity with the number of images increasing.

In order to solve the problem, a multi-image encryption using spherical diffraction and filtering diffusion is proposed. Owing to the asymmetric characteristics of spherical diffraction, the proposed encryption can effectively resist the phase retrieval attack. Moreover, each image can be decrypted individually with its private key, which has high decryption flexibility. The most significant advantage of this algorithm is the super-large encryption capacity. The encryption capacity is the product of image resolution and grayscale level, which is super-large of $2^8 \times m \times n$ in case of $m \times n$ points of an image with 2^8 grayscale level. Numerical simulation results verify the feasibility and effectiveness of the proposed encryption.

The rest of this paper is organized as follows. Section 2 introduces the spherical diffraction and filtering diffusion technology. Section 3 presents principle of encryption and decryption. Section 4 shows simulation results. Section 5 draws a conclusion.

2. Principles of the Method

2.1. Encryption in Spherical Diffraction Domain

Since spherical diffraction (SpD) is an asymmetry diffraction propagation model [38], the SpD-based encryption should overcome the shortage of symmetry cryptosystem, which is based on traditional diffraction. According to the spherical diffraction theory [38–42], the object and the observation surfaces are concentric spheres. r and R represent the radii of the inner and outer surfaces of the concentric sphere, respectively. In this diffraction model, there are two models of propagation, namely the inside-out propagation (IOP) model and the outside-in propagation (OIP) model, as shown in Figure 1a,b, respectively.

Figure 1. Spherical diffraction model: (a) inside-out propagation (IOP) model, (b) outside-in propagation (OIP) model.

We use $Q_R(\theta_R, \varphi_R)$ and $P_r(\theta_r, \varphi_r)$ in the spherical coordinates to denote the object and the observation points for the OIP model, respectively. The spherical coordinate of $Q_r(\theta_r, \varphi_r)$ and $P_R(\theta_R, \varphi_R)$ denote the object and the observation points for the IOP model, respectively. θ_r and θ_R are in the range of $-\pi$ to π , φ_r and φ_R are in the range of $-\pi/2$ to $\pi/2$. If we represent the diffraction

distributions on the inner and outer surfaces by $u_r(\theta_r, \varphi_r)$ and $u_R(\theta_R, \varphi_R)$, the diffraction integral formulas based on the Rayleigh–Sommerfeld integral equation of the two models can be written as

$$u_r(\theta_r, \varphi_r) = C \iint_s u_R(\theta_R, \varphi_R) \cos \alpha \frac{\exp(ikd_{ORPr})}{d_{ORPr}} d\theta_R d\varphi_R = SpD_r(u_r(\theta_r, \varphi_r)) \dots \dots \text{OIP}, \quad (1)$$

$$\cos \alpha = \frac{r - R \cos(\theta_R - \theta_r) \cos(\varphi_R - \varphi_r)}{d_{ORPr}}, \quad (2)$$

$$d = d_{ORPr} = d_{OrPR} = \sqrt{r^2 + R^2 - 2Rr \cos(\theta_R - \theta_r) \cos(\varphi_R - \varphi_r)}, \quad (3)$$

$$u_R(\theta_R, \varphi_R) = C \iint_s u_r(\theta_r, \varphi_r) \frac{\exp(ikd_{OrPR})}{d_{OrPR}} d\theta_r d\varphi_r = SpD_R(u_R(\theta_R, \varphi_R)) \dots \dots \text{IOP}, \quad (4)$$

where C denotes a constant and k denotes the wavenumber of the incident light. d denotes the distance between two points of P and Q on the object and observation surfaces. s represents the object surface.

2.2. Filtering Diffusion Technology

Image filtering is a digital image processing technology, which is mainly used to eliminate image noise or extract image features. The method performs convolution operation on a 2D image block and a 2D matrix, named kernel. To be specific, the additions of all the multiplications of the kernel pixels and image pixels are used as the value of the current pixel. The current pixel value corresponds to the center element of kernel, and the other elements correspond to adjacent pixels. R is the selected image block, the central pixel $R_{x,y}$ is the pixel to be processed, and M is the kernel. Assuming the kernel size is $(2n + 1) \times (2n + 1)$, the calculation of image filtering can be defined as

$$R'_{x,y} = \sum_{i=-n}^n \sum_{j=-n}^n M_{i+n+1,j+n+1} R_{x+i,y+j}. \quad (5)$$

Selecting a suitable kernel to filter can emphasize some features or remove unwanted parts in the image. However, we can also use a randomly generated kernel to diffuse the image for encryption. Since the slight change of the current pixel would affect the value of each subsequent pixel, it has a good diffusion effect.

To make the filtering invertible, we set the center pixel of the kernel as one and set other pixels as integers. To get a better diffusion effect, the lower-right corner of the kernel is set to correspond to the current pixel, namely $M_{2n+1,2n+1} = 1$. The current pixel $R_{x,y}$ is processed by the upper and left adjacent pixels. Figure 2 shows the filtering diffusion process.

Figure 2. The filtering diffusion process.

According to filtering diffusion theory [43,44], the calculation of filtering diffusion can be expressed as

$$R'_{x,y} = \left(\sum_{i=-n}^n \sum_{j=-n}^n M_{i+n+1,j+n+1} R_{x+i,y+j} \right) \bmod F, \quad (6)$$

$$R_{x,y} = \left(R'_{x,y} - \sum_{i,j \in \{-n,\dots,n\} \cap (i,j) \neq (0,0)} M_{i+n+1,j+n+1} R_{x+i,y+j} \right) \bmod F. \quad (7)$$

Before filtering the current pixel, the upper and left pixels should be processed. When doing inverse filtering, it is also required that the upper and left adjacent pixels have not been restored. Therefore, the processing order of inverse filtering should be reversed from that of the forward operation.

3. Principle of Encryption and Decryption

In the process of encryption, filtering diffusion and chaotic scrambling are first used to diffuse and scramble encrypted images, respectively. Second, multiple images are superimposed together using the XOR operation. Then, the superimposed image is transformed into the spherical diffraction domain. Finally, the improved equal modulus decomposition (EMD) is employed to obtain ciphertext and private key. The process of decryption is the inverse operation of encryption.

3.1. Process of Encryption

The multi-image encryption based on filtering diffusion and spherical diffraction is shown in Figure 3. Suppose the original gray images are represented by $I_N(x, y)$, the proposed method can be described as follows:

Figure 3. Process of encryption.

Step 1: First, the images are processed by filtering diffusion using the 2D kernel of size 2×2 individually. We set $M_{2,2}$ as one, and the other three numbers are randomly generated integers from 0 to 255. In the filtering diffusion process, the leftmost column and the topmost row of the image do not have enough pixels for calculation. Hence, the rightmost and bottommost pixels can be used for expansion [43]. Starting from the upper left corner of the image, each pixel is processed in turn. The processed pixel value can be expressed as

$$I'_N(x, y) = \left(\sum_{i,j \in \{1,2\}} M(i, j) I_N(i, j) \right) \bmod F, \quad (8)$$

where F denotes the grayscale level.

Step 2: To get a better encryption effect, the images are scrambled by the chaotic sequence individually. The chaotic sequence is obtained by

$$x_{n+1} = \mu x_n(1 - x_n). \quad (9)$$

The range of x_n is (0, 1) and the range of μ is (0, 4).

Step 3: Combining the images into one image using the XOR operation. The superimposed result can be written as

$$f(x, y) = I'_1(x, y) \oplus I'_2(x, y) \dots \oplus I'_N(x, y). \quad (10)$$

At the same time, P_N can be obtained by

$$P_N(x, y) = f(x, y) \oplus I'_N(x, y), \quad (11)$$

where P_N is reserved as the private key of each image for decryption.

Step 4: The combined image $f(x, y)$ is mapped on the spherical surface with a radius of R after it is modulated by the random phase mask $RPM(x, y) = \exp[iR_1(x, y)]$. R_1 is a random array uniformly distributed between 0 and 2π . According to the OIP model, the modulated image is transformed into a spherical coordinate. If we use $U(x, y)$ to represent the complex amplitude after spherical diffraction, the expression can be written as

$$U(x, y) = SpD_R[f(x, y)RPM(x, y)]. \quad (12)$$

Step 5: To improve the anti-attack ability, we use the improved EMD [45] to decompose complex amplitude. The distribution of complex amplitude can be written as

$$U = A \times \exp(i\beta) = C \times [\exp(iR_2) + \exp(iPK)], \quad (13)$$

$$R_2 = 2\pi \times \text{rand}(), \quad (14)$$

where A is the amplitude and β represents the phase of U , $\text{rand}()$ denotes a random function. The ciphertext C and the private key PK can be expressed as follows:

$$C = 0.5A \times [\cos(\beta - R_2)]^{-1}, \quad (15)$$

$$PK = 2\beta - R_2, \quad (16)$$

where the ciphertext C and the private key PK are both real-valued, so that they are convenient for recording and transmission.

3.2. Process of Decryption

Figure 4 shows process of decryption. The detailed steps are as follows:

Step 1: According to the Equation (13), we can get the complex amplitude U . The U is modulated by RPM^* after spherical diffraction. The combined image $f(x, y)$ can be obtained by

$$f(x, y) = ISpD[U(x, y)]RPM^*, \quad (17)$$

where $ISpD[\bullet]$ represents the inverse process of the spherical diffraction calculation. Then $f(x, y)$ is rounded to unify the data types.

Step 2: Based on the Equation (11), image $I'_N(x, y)$ can be obtained by

$$I'_N(x, y) = f(x, y) \oplus P_N(x, y). \quad (18)$$

Step 3: According to the Equation (8), the decrypted images can be obtained by the inverse chaotic scrambling and the inverse filtering diffusion in this scheme.

Figure 4. Process of decryption.

4. Simulation Results

4.1. Encryption and Decryption Results

The numerical simulation for the proposed encryption has been carried out on a PC with Intel (R) Core(TM) i5-7200U CPU 2.50 GHz and 8 GB memory capacity. Python 3.7 is used for this numerical simulation. The outer spherical R , inner spherical r and the wavelength λ are set as 500×10^{-3} m, 50×10^{-3} m and 250×10^{-6} m, respectively, as shown in Table 1. According to the sampling theorem in the spherical diffraction calculation [41], the pixel numbers in the azimuthal and vertical directions are at least 2514 and 1257, respectively. If we take 1/5 of the surface for spherical diffraction, the minimum number of pixels required in the azimuthal and vertical directions are 503 and 252, respectively. Therefore, the size of the original image is selected as 512×512 pixels. Figure 5a–d show the original images with 512×512 pixels for the proposed method. Figure 5e,f shows the private key of the first image P_1 and the combined image f , respectively. Figure 5g,h shows the ciphertext C and the private key PK , respectively. Figure 5a1–d1 shows decrypted images with correct keys.

Table 1. The algorithm's parameters.

R	r	λ	x_n	μ
500×10^{-3} m	50×10^{-3} m	250×10^{-6} m	0.50	3.70

To evaluate the decryption quality, the peak signal-to-noise (PSNR) and the correlation coefficient (CC) between the decrypted and original images are calculated. The formula of PSNR and CC can be given by

$$PSNR(I_o, I_d) = 10 \log_{10} \left[\frac{M \times N \times 255^2}{\sum_{x,y} [I_o(x,y) - I_d(x,y)]^2} \right], \quad (19)$$

$$CC = \frac{E\{[I_o - E[I_o]][I_d - E[I_d]]\}}{\sqrt{E\{[I_o - E[I_o]]^2\}} \sqrt{E\{[I_d - E[I_d]]^2\}}}, \quad (20)$$

where $M \times N$ is the size of image and $E\{\bullet\}$ denotes the expected value of the function, I_o and I_d represent the original and decrypted images, respectively. The PSNR and the CC values between the original images and corresponding decrypted images are infinity and 1, respectively, which shows the decrypted images are lossless.

Figure 5. Encryption and decryption results: (a–d) original images, (e) private key for the first image P_1 , (f) combined image f , (g) ciphertext C , (h) private key PK , (a1–d1) decrypted images.

4.2. Key Sensitivity and Key Space Analysis

The key sensitivity is usually used to test whether the proposed method is stable. For brevity, only the decryption image “cameraman” is shown. The dependences of CC on the change of r , R , and λ are shown in Figure 6. When r , R , and λ value changes 2×10^{-6} , 4×10^{-6} , 4×10^{-9} respectively, CC value would change dramatically. It shows that this method is extremely sensitive to the keys. From the above analysis, the key space of this method is $(10^6)^3 = 10^{18}$.

Figure 6. Correlation coefficient (CC) values of decrypted images with incorrect keys: (a) $\Delta r/\Delta R$ (mm/100), (b) $\Delta \lambda$ ($\mu\text{m}/100$).

4.3. Histogram

The histogram shows the effectiveness and security of the encryption. The ideal histogram should be almost different from the original image. The histograms of original images are shown in Figure 7a–d, respectively. Figure 7e shows the histogram of the encrypted image, which is very different from the original image. Figure 7f shows the other encrypted image using different original images, which is similar to Figure 7e.

Figure 7. Histogram: (a–d) original images, (e) encrypted image, (f) encrypted image using different original images.

4.4. Adjacent Pixel Correlation

Table 2 shows the adjacent pixels correlation of the four original images, the encrypted image and the encrypted image in other multi-image encryption method. An efficient encryption should significantly reduce the adjacent pixel correlation of the original images. It can be defined as

$$CC(X, Y) = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y}, \quad (21)$$

where X and Y are two different pixel sequences, in which each pixel is the adjacent pixel of X . μ and σ denote the mean value and the standard derivation, respectively. $E[\bullet]$ represents the mathematical expectation.

Table 2. Adjacent pixel correlation.

Correlation Coefficient	Horizontal	Vertical	Diagonal
cameraman	0.966649	0.978250	0.978232
peppers	0.973320	0.976367	0.980875
baboon	0.879297	0.799324	0.799965
coco	0.989351	0.990687	0.990696
ciphertext	0.000046	0.000203	0.002142
Ref. [36]	0.002800	0.034100	−0.054700
Ref. [22]	−0.026800	0.013500	0.010300
Ref. [23]	0.025300	0.019700	0.026900

Table 2 shows that the correlation between adjacent pixels of the ciphertext is much lower than that of the original images, and it's also lower than the results of other methods.

4.5. Noise and Occlusion Attacks

Images are susceptible to noise pollution during transmission. It is necessary to ensure that the encryption has a certain anti-noise attack capability. In this section, the multiplicative noise is added to the encrypted image to test the effects of noise. The multiplicative noise model is given by

$$P' = P(1 + kG), \quad (22)$$

where P and P' denotes the encrypted image and the encrypted image with noise, respectively. G represents the white Gaussian noise with zero-mean and 0.01 standard deviation, k represents the noise strength.

Figure 8 shows the decrypted results of the encrypted image with different strength noise. Figure 8a–c shows the results of the intensity $k = 0.05, 0.07, 0.10$, respectively, and the corresponding PSNR values are 30.96, 27.07, 24.36 dB, respectively.

Figure 8. The decrypted results of the encrypted image with different strength noise: (a) $k = 0.05$, (b) $k = 0.07$, (c) $k = 0.10$.

Figure 9a–c shows the decryption results of the ciphertext center being occluded by 4×4 , 6×6 , 8×8 pixels, respectively, and the corresponding PSNR values are 31.24, 25.51, 24.00 dB, respectively.

Figure 9. The decrypted results of the encrypted image with different pixels occlusion: (a) 4×4 , (b) 6×6 , (c) 8×8 .

4.6. Potential Attack Analysis

Usually, if the encryption can resist the chosen-plaintext attack, it can resist other common attacks. Based on the proposed method, the illegal user uses the encryption to encrypt arbitrary images to obtain fake private keys, which would be used to decrypt the original image. At the same time, the encryption key such as R, r, λ , and the 2D kernel is known by the illegal user. Figure 10a–d shows the decrypted image, which doesn't have any information about the original image. It shows that the proposed method can resist the chosen-plaintext attack.

Figure 10. Decryption results of chosen-plaintext attack without key (a) R, (b) r, (c) λ , (d) 2D kernel.

Phase retrieval attack is usually used to test the security of the encryption method. Figure 11 shows the relation between the CC value of the combined image and iteration numbers. It shows that the CC value quickly converges to around 0 with the increase of iteration numbers, which indicates that the proposed method can resist phase retrieval attack effectively.

Figure 11. CC values change along with the iteration number.

An encryption system with good encryption effect should be able to resist differential attack. Generally, the number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used to evaluate the ability to resist the differential attack, which are defined as follows:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N D(i, j) \times 100\%, \quad (23)$$

$$D(i, j) = \begin{cases} 1, E(i, j) \neq E'(i, j) \\ 0, E(i, j) = E'(i, j) \end{cases} \quad (24)$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N \frac{|E(i, j) - E'(i, j)|}{255} \times 100\%, \quad (25)$$

where E and E' are two ciphertexts, generated from two original images that have only one different pixel, and $M \times N$ is the size of image. To obtain NPCR and UACI, we choose one of the images to change a random pixel, and encrypt them with the same key. The results of NPCR and UACI are shown in Table 3. It shows that the proposed encryption can resist differential attack very well.

Table 3. The values of the number of pixel change rate (NPCR) and unified average changing intensity (UACI).

Image	NPCR (%)	UACI (%)
cameraman	99.6046	33.1825
peppers	99.6046	33.9021
baboon	99.6046	33.3199
coco	99.6046	34.1323

4.7. Time and Computational Complexity Analysis

In this analysis, we use the original images of size 265×256 and 512×512 to test the time to encrypt different numbers of images. The results are shown in Table 4. It shows that as the number of encryption increases, the encryption time also increases. At the same time, the computational complexity of the proposed encryption is $O(n^2)$.

Table 4. The time of encrypting different numbers of images.

Size	One Image	Two Images	Three Images	Four Images
256×256	0.6393 s	1.2354 s	1.8577 s	2.4489 s
512×512	2.5149 s	4.9587 s	7.4733 s	9.7806 s

4.8. Capacity of Image Encryption

For a multi-image encryption, the number of encryption images is an essential indicator of measurement. In this proposed encryption, the bit-wise XOR operation for two images will maintain the pixel value range of original images. That is, the pixel value of the original images is in the range of 0–255, and the pixel value of the combined image is still in the range of 0–255 after using the XOR operation. Therefore, multi-image encryption through XOR multiplexing should have no decryption crosstalk theoretically. Since the private key of each different image generated in the encryption process must be different, the encryption capacity is limited by the maximum number of possible private keys, which is the product of the maximum grayscale level and the resolution of the private key image. Therefore, the encryption capacity EC can be expressed as

$$EC = 2^w \times m \times n, \quad (26)$$

where w represents the bit-depth of the encrypted image, $m \times n$ represents the size of the encrypted image. If the size of the encrypted image is $m \times n$, and the grayscale level is 8, the encryption capacity would be $2^8 \times m \times n$.

We preprocess the images to ensure that each image is different. Figure 12 shows the decryption results of 200, 500, 1000, and 2000 different images with 64×64 pixels and their CC values, respectively. It can be seen that the decryption quality is still excellent when the number of encryption images reaches 2000. This indicates that the proposed encryption breaks through the number limitation of the conventional multi-image encryptions and greatly increases their encryption capacity.

Figure 12. Decryption results of 200, 500, 1000, and 2000 different images with 64×64 pixels and their CC value.

5. Conclusions

In this article, we propose a large-capacity multi-image encryption using spherical diffraction and filtering diffusion. In this encryption, original images are combined into one image using the XOR operation after filtering diffusion. Then, the superimposed image is transformed into the spherical diffraction domain and encrypted by the improved EMD. Due to the remainder operation in the XOR operation, the range of the combined image is always maintained in the original image range, which would not exceed the limitation of image range or cause data crosstalk. Therefore, the encryption capacity is the product of image resolution and grayscale level, which is super-large of $2^8 \times m \times n$ in case of $m \times n$ points of an image with 2^8 grayscale level. Moreover, the proposed method is highly flexible due to individual decryption with the individual private key for each plaintext image. Besides, it can resist phase-retrieval attack due to the asymmetry of spherical diffraction. The encryption system significantly increases the capacity of the multi-image encryption system, though it has weak anti-occlusion ability. In further work, the encryption method can be used in the color multi-image encryption system. The feasibility and effectiveness of the proposed encryption have been demonstrated by the simulation results.

Author Contributions: Conceptualization, H.W. and J.W.; methodology, H.W.; software, H.W., X.C. and Z.Z. (Zheng Zhu); validation, H.W. and J.W.; formal analysis, Z.Z. (Ziyi Zhang); investigation, J.W.; resources, H.W.; data curation, H.W.; writing—original draft preparation, H.W.; writing—review and editing, J.W. and Z.Z. (Ziyi Zhang); supervision, J.W.; project administration, J.W.; funding acquisition, J.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (NSFC) (U1933132) and the Chengdu Science and Technology Program (2019-GH02-00070-HZ).

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

References

1. Liu, S.T.; Mi, Q.L.; Zhu, B.H. Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. *Opt. Lett.* **2001**, *26*, 1242–1244. [\[CrossRef\]](#) [\[PubMed\]](#)
2. Qin, Y.; Wang, Z.P.; Wang, H.J.; Gong, Q. Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code. *Opt. Lasers Technol.* **2018**, *103*, 93–98. [\[CrossRef\]](#)
3. Zhou, N.R.; Pan, S.M.; Cheng, S.; Zhou, Z.H. Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. *Opt. Lasers Technol.* **2016**, *82*, 121–133. [\[CrossRef\]](#)
4. Chang, K.-M.; Chen, C.; Wang, J.; Wang, Q.-H. Improved single-random-phase holographic encryption using double-phase method. *Opt. Commun.* **2019**, *443*, 19–25. [\[CrossRef\]](#)
5. Dou, Y.Q.; Li, M. Cryptanalysis of a New Color Image Encryption Using Combination of the 1D Chaotic Map. *Appl. Sci.* **2020**, *10*, 2187. [\[CrossRef\]](#)
6. Zhu, Z.; Chen, X.D.; Wu, C.; Wang, J.; Wang, W.X. An asymmetric color-image cryptosystem based on spiral phase transformation and equal modulus decomposition. *Opt. Lasers Technol.* **2020**, *126*, 106106. [\[CrossRef\]](#)

7. Catak, F.O.; Aydin, I.; Elezaj, O.; Yildirim-Yayilgan, S. Practical Implementation of Privacy Preserving Clustering Methods Using a Partially Homomorphic Encryption Algorithm. *Electronics* **2020**, *9*, 229. [\[CrossRef\]](#)
8. Refregier, P.; Javidi, B. Optical-Image Encryption Based on Input Plane and Fourier Plane Random Encoding. *Opt. Lett.* **1995**, *20*, 767–769. [\[CrossRef\]](#)
9. Frauel, Y.; Castro, A.; Naughton, T.J.; Javidi, B. Resistance of the double random phase encryption against various attacks. *Opt. Express* **2007**, *15*, 10253–10265. [\[CrossRef\]](#)
10. Peng, X.; Zhang, P.; Wei, H.Z.; Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **2006**, *31*, 1044–1046. [\[CrossRef\]](#)
11. Peng, X.; Wei, H.Z.; Zhang, P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Opt. Lett.* **2006**, *31*, 3261–3263. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Chen, W.; Chen, X.D. Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain. *Opt. Commun.* **2011**, *284*, 3913–3917. [\[CrossRef\]](#)
13. Wang, J.; Wang, Q.H.; Hu, Y.H. Image Encryption Using Compressive Sensing and Detour Cylindrical Diffraction. *IEEE Photonics J.* **2018**, *10*, 1–4. [\[CrossRef\]](#)
14. Ding, X.L.; Huang, Y.M.; Zhang, D.Y.; Song, Y. Nonlinear Double-Image Encryption in Cylindrical Diffraction-Based Scheme by Aid of Position Multiplexing. *IEEE Access* **2020**, *8*, 205–214. [\[CrossRef\]](#)
15. Wang, J.; Li, X.; Hu, Y.; Wang, Q.-H. Phase-retrieval attack free cryptosystem based on cylindrical asymmetric diffraction and double-random phase encoding. *Opt. Commun.* **2018**, *410*, 468–474. [\[CrossRef\]](#)
16. Singh, H.; Yadav, A.K.; Vashisth, S.; Singh, K. Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane. *Opt. Lasers Eng.* **2015**, *67*, 145–156. [\[CrossRef\]](#)
17. Zhou, N.R.; Li, H.L.; Wang, D.; Pan, S.M.; Zhou, Z.H. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. *Opt. Commun.* **2015**, *343*, 10–21. [\[CrossRef\]](#)
18. Hwang, H.-E.; Chang, H.T.; Lie, W.-N. Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain. *Opt. Lett.* **2009**, *34*, 3917–3919. [\[CrossRef\]](#)
19. Gao, Y.; Jiao, S.M.; Fang, J.C.; Lei, T.; Xie, Z.W.; Yuan, X.C. Multiple-image encryption and hiding with an optical diffractive neural network. *Opt. Commun.* **2020**, *463*, 125476. [\[CrossRef\]](#)
20. Sui, L.S.; Zhang, L.W.; Wang, Q.; Tian, A.L.; Anand, A. Multiple-image authentication based on the single-pixel correlated imaging and multiple-level wavelet transform. *Opt. Lasers Eng.* **2020**, *130*, 106102.
21. Xi, S.X.; Yu, N.N.; Wang, X.L.; Wang, X.G.; Lang, L.Y.; Wang, H.Y.; Liu, W.W.; Zhai, H.C. Optical encryption scheme for multiple-image based on spatially angular multiplexing and computer generated hologram. *Opt. Lasers Eng.* **2020**, *127*, 105953. [\[CrossRef\]](#)
22. Sui, L.; Zhang, X.; Tian, A. Multiple-Image Hiding Based on Cascaded Free-Space Wave Propagation Using the Structured Phase Mask for Lensless Optical Security System. *IEEE Photonics J.* **2017**, *9*, 1–14. [\[CrossRef\]](#)
23. Zhang, L.; Yuan, X.; Wang, K.; Zhang, D. Multiple-Image Encryption Mechanism Based on Ghost Imaging and Public Key Cryptography. *IEEE Photonics J.* **2019**, *11*, 1–14. [\[CrossRef\]](#)
24. Wu, C.; Wang, Y.; Chen, Y.; Wang, J.; Wang, Q.-H. Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain. *Opt. Commun.* **2019**, *431*, 203–209. [\[CrossRef\]](#)
25. Kong, D.Z.; Shen, X.J.; Xu, Q.Z.; Xin, W.; Guo, H.Q. Multiple-image encryption scheme based on cascaded fractional Fourier transform. *Appl. Opt.* **2013**, *52*, 2619–2625. [\[CrossRef\]](#)
26. Wang, X.G.; Zhao, D.M. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain. *Opt. Commun.* **2011**, *284*, 148–152. [\[CrossRef\]](#)
27. Liansheng, S.; Xiao, Z.; Chongtian, H.; Ailing, T.; Krishna Asundi, A. Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. *Opt. Lasers Eng.* **2019**, *113*, 29–37. [\[CrossRef\]](#)
28. Li, Y.B.; Zhang, F.; Li, Y.C.; Tao, R. Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform. *Opt. Lasers Eng.* **2015**, *72*, 18–25. [\[CrossRef\]](#)
29. Gong, Q.; Liu, X.Y.; Li, G.Q.; Qin, Y. Multiple-image encryption and authentication with sparse representation by space multiplexing. *Appl. Opt.* **2013**, *52*, 7486–7493. [\[CrossRef\]](#)
30. Shi, Y.; Zhang, J. Research on the phase retrieval algorithm used for multiple-image encryption with region multiplexing. *Guangxue Xuebao Acta Opt. Sin.* **2009**, *29*, 2705–2708. [\[CrossRef\]](#)

31. Situ, G.H.; Zhang, J.J. Multiple-image encryption by wavelength multiplexing. *Opt. Lett.* **2005**, *30*, 1306–1308. [[CrossRef](#)] [[PubMed](#)]
32. He, X.L.; Tao, H.; Jiang, Z.L.; Kong, Y.; Wang, S.Y.; Liu, C. Single-shot optical multiple-image encryption by jointly using wavelength multiplexing and position multiplexing. *Appl. Opt.* **2020**, *59*, 9–15. [[CrossRef](#)] [[PubMed](#)]
33. Liu, L.; Shan, M.; Zhong, Z.; Liu, B. Multiple-image encryption and authentication based on optical interference by sparsification and space multiplexing. *Opt. Lasers Technol.* **2020**, *122*, 105858. [[CrossRef](#)]
34. Deepan, B.; Quan, C.; Wang, Y.; Tay, C.J. Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. *Appl. Opt.* **2014**, *53*, 4539–4547. [[CrossRef](#)]
35. Zhao, H.Z.; Liu, J.; Jia, J.; Zhu, N.; Xie, J.H.; Wang, Y.T. Multiple-image encryption based on position multiplexing of Fresnel phase. *Opt. Commun.* **2013**, *286*, 85–90. [[CrossRef](#)]
36. Hu, K.-Y.; Wu, C.; Wang, Y.; Wang, J.; Wang, Q.-H. An asymmetric multi-image cryptosystem based on cylindrical diffraction and phase truncation. *Opt. Commun.* **2019**, *449*, 100–109. [[CrossRef](#)]
37. Liu, Z.; Liu, S. Double image encryption based on iterative fractional Fourier transform. *Opt. Commun.* **2007**, *275*, 324–329. [[CrossRef](#)]
38. Wang, J.; Wang, Q.-H. *Outside-in Propagation Model for Spherical Computer-Generated Hologram*, International Workshop on Holography and Related Technologies; IWH: Beijing, China, 2014.
39. Jackin, B.J.; Yatagai, T. Fast calculation of spherical computer generated hologram using spherical wave spectrum method. *Opt. Express* **2013**, *21*, 935–948. [[CrossRef](#)]
40. Li, G.; Phan, A.H.; Kim, N.; Park, J.H. Synthesis of computer-generated spherical hologram of real object with 360 degrees field of view using a depth camera. *Appl. Opt.* **2013**, *52*, 3567–3575. [[CrossRef](#)]
41. Tachiki, M.L.; Sando, Y.; Itoh, M.; Yatagai, T. Fast calculation method for spherical computer-generated holograms. *Appl. Opt.* **2006**, *45*, 3527–3533. [[CrossRef](#)]
42. Li, G.; Hong, K.; Yeom, J.; Chen, N.; Park, J.H.; Kim, N.; Lee, B. Acceleration method for computer generated spherical hologram calculation of real objects using graphics processing unit. *Chin. Opt. Lett.* **2014**, *12*, 060016.
43. Hua, Z.; Zhou, Y. Design of image cipher using block-based scrambling and image filtering. *Inf. Sci.* **2017**, *396*, 97–113. [[CrossRef](#)]
44. Hua, Z.; Xu, B.; Jin, F.; Huang, H. Image Encryption Using Josephus Problem and Filtering Diffusion. *IEEE Access* **2019**, *7*, 8660–8674. [[CrossRef](#)]
45. Wang, J.; Chen, X.; Zeng, J.; Wang, Q.-H.; Hu, Y. Asymmetric Cryptosystem Using Improved Equal Modulus Decomposition in Cylindrical Diffraction Domain. *IEEE Access* **2019**, *7*, 66234–66241. [[CrossRef](#)]

© 2020 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 (<http://creativecommons.org/licenses/by/4.0/>).