entropy

MDPI

Article

Multi-Image Encryption Method via Computational Integral Imaging Algorithm

Xiaowu Li [1], Chuying Yu [2,*] and Junfeng Guo [3,*]

[1] The Second Affiliated Hospital of Shantou University Medical College , Shantou 515000, China; lxw_841121@163.com
[2] School of Physics and Electronic Engineering, Hanshan Normal University, Chaozhou 521041, China
[3] School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China
* Correspondence: chyyu@hstc.edu.cn (C.Y.); gjf_200200110@126.com (J.G.)

Abstract: Under the framework of computational integral imaging, a multi-image encryption scheme based on the DNA-chaos algorithm is proposed. In this scheme, multiple images are merged to one image by a computational integral imaging algorithm, which significantly improves the efficiency of image encryption. Meanwhile, the computational integral imaging algorithm can merge images at different depth distances, thereby the different depth distances of multiple images can also be used as keys to increase the security of the encryption method. In addition, the high randomness of the chaos algorithm is combined to address the outline effect caused by the DNA encryption algorithm. We have experimentally verified the proposed multi-image encryption scheme. The entropy value of the encrypted image is 7.6227, whereas the entropy value of the merge image with two input images is 3.2886, which greatly reduces the relevance of the image. The simulation results also confirm that the proposed encryption scheme has high key security and can protect against various attacks.

Keywords: multi-image encryption; computational integral imaging; DNA-chaos algorithm

check for updates

Citation: Li, X.; Yu, C.; Guo, J. Multi-Image Encryption Method via Computational Integral Imaging Algorithm. *Entropy* **2022**, *24*, 996. https://doi.org/10.3390/e24070996

Academic Editors: Jiayi Ma and Amelia Carolina Sparavigna

Received: 6 May 2022
Accepted: 12 July 2022
Published: 18 July 2022

1. Introduction

As a basic way of carrying data, the importance of images in the information industry is self-evident. However, there is no doubt that this will raise a lot of privacy concerns if the image information owned by an individual or team is accessed by others. Image encryption is a proven means of solving image security problems [1–6]. Encrypted images lack intuitive information about the original image, in other words, the thief cannot obtain any valuable information from the encrypted image, thereby achieving the privacy protection of the image owner. At present, researchers have proposed many methods of image encryption, and optical encryption has attracted much attention in the study of image encryption because of its unique multi-dimensional capabilities, high parallelism and high-speed processing power [7–12].

Since Javidi and Refregier proposed the classic optical Dual Random Phase Encoding (DRPE) system in 1995 [13], optical encryption technology began to enter a period of rapid development. Researchers have found that the encryption system based on DRPE technology has some security problems due to its own linear factors [14]; it is vulnerable to selective plaintext attacks. In order to enhance the security of the encryption system, researchers have proposed a series of feasible optical encryption improvement schemes based on DRPE. The improvements are mainly made from the following four aspects: (1) Expansion of optical transformations; (2) Pre-process according to the characteristics of the encrypted image and the purpose of encryption; (3) Improvements of the random phase mask; (4) Non-linear operation. On this basis, more encryption algorithms have been proposed [15–20]. It is worth noting that these proposed methods of encrypting objects are all for a single image. Compared with single image encryption, multi-image encryption can process multiple images at a time, which can greatly improve encryption efficiency on the basis of ensuring encryption security.

Computational Integral Imaging (CII), as a well-performing optical imaging system, can achieve a full-color, wide-angle 3D light field display [21–27]. Integral imaging technology can record image information from multiple perspectives of a scene, which can provide more robustness in the recovery process of image encryption. Researchers have proposed many image encryption methods based on the CII framework, and confirmed that these algorithms have strong robustness [28–30]. In addition, computational integral imaging technology can also record scene information at different depths; at the same time [31–33], it is possible to achieve the synthesis of multiple images, which provides a new idea for multi-image encryption.

DNA algorithm with vast parallelism, large-scale storage and extraordinary information density is often applied in the study of data encoding, and some DNA-based encoding algorithms were proposed and showed a better performance [34–39]. The proposed DNA-based encryption algorithms have two main ideas—one is to explore the impact of different DNA rules on encryption performance, and the other is to improve the performance of DNA encryption by combining other encryption algorithms [40]. There will be an outline effect when DNA encryption algorithm is used, which causes the saliency boundaries of the original image to be seen from the encrypted image clearly. The chaos system possesses a variety of characteristics, such as strong confidentiality, good randomness, a large amount of keys and so on [41–43]. In addition, recently, elliptic curves-based image encryption schemes have been considered an alternative to the chaos-based schemes [44–47]. Therefore, they are widely used in combination with DNA algorithms to improve the performance of encryption systems.

In this paper, a multi-image encryption scheme based on CII using a DNA-chaos encryption algorithm is proposed. Two or more images are merged in different depths using the CII algorithm, which will obtain an Element Image Array (EIA) image, and then the EIA image is encrypted by the DNA-chaos encryption algorithm. Finally, the decrypted image can be reconstructed at different depths to restore the original image. Based on the high security of the DNA-chaos encryption algorithm, EIA data recorded by computational integral imaging technology to ensure the strong robustness and the multi-image merge scheme of different depths further improves the key space by using depth information as the key.

The paper is arranged as follows. In Section 2, we briefly introduce a theoretical analysis of our method, including the CII pickup process, DNA sequence operations, chaos theory, the CII Reconstruction (CIIR) algorithm and entropy analysis theory. A multi-image encryption scheme is proposed in Section 3. In Section 4, we analyze the performance of the proposed multi-image encryption scheme in terms of key security, statistical results, robustness and time analysis. The conclusions reached in this article are presented in Section 5.

2. Previous Theoretical Analysis

2.1. Pickup Original Scene by CII

CII [22] is an advanced optical imaging solution, which is the most promising commercial 3D display technology, and has important research significance in the field of 3D image processing. The modulation of optical information from CII mainly includes two processes—one is the pickup of the original scene, which can obtain the EIA, and the other is the reconstruction of the original scene through EIA. In the pickup of the original scene, an EIA is recorded, and the EIA contains a lot of redundant information about the scene, which can improve the robustness of the encryption scheme for image encryption.

Figure 1 shows the pickup of the original scene by CII algorithm. The original scene is recorded by the sensor as EIA through a lenslet array, and the EIA contains many EIs; each EI represents the encrypted information converted by part of the original scene. Each EI is calculated by [22]:

$$E(x,y,z) = P\left(-\frac{xd}{l} + i\phi, -\frac{yd}{l} + j\phi, z\right), \tag{1}$$

where x, y and z represent the spatial coordinates of the lenslet array, and the size of the lenslet array determines the number of EIs. ϕ represents the size of lens, and the distance from image to lenslet array is l.

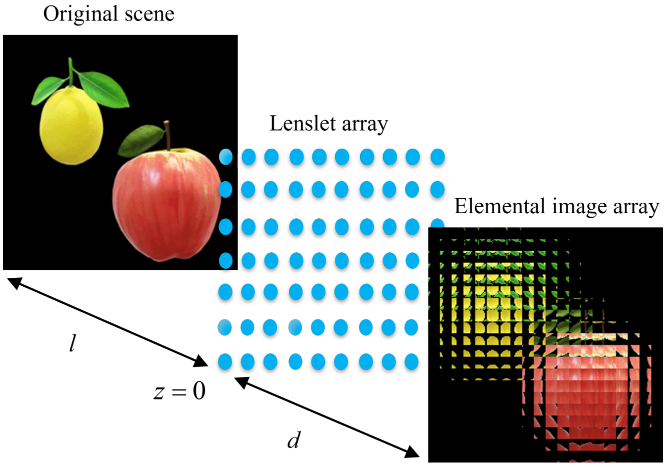

Figure 1. The pickup of the original scene by CII.

2.2. DNA Sequence Operations

A Deoxyribo Nucleic Acid (DNA) sequence consists of four different basic nucleotides: adenine (A), guanine (G), thymine (T) and cytosine (C). These four nucleotides can be combined to form a long sequence, and T is paired with A,G is paired with C. We will obtain 24 different encoding schemes if A,C,G and T are encoded as binary numbers with two bits, respectively, but only eight encoding schemes suit the Watson–Crick rule, and they are shown in Table 1. Assuming that A-10, T-01, C-11, G-00, such as the binary sequence 10110100, the DNA sequence can be written as ACTG.

Table 1. DNA coding rules.

Rule	One	Two	Three	Four	Five	Six	Seven	Eight
A	00	00	01	01	10	10	00	11
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01
T	11	11	10	10	01	01	00	00

DNA computing has received a lot of attention from researchers, so it has developed rapidly. Some researchers have proposed certain algebraic operations for DNA sequences, such as addition operations, subtraction operations and Ex-OR operations. Corresponding to the eight DNA coding schemes there are also eight DNA addition, subtraction and Ex-OR operations. Table 2 lists one of the arithmetic rules which, according to DNA encoding rule one, are listed in Table 1 [34].

Table 2. DNA addition, subtraction and XOR operations.

+	A	T	C	G	-	A	T	C	G	⊕	A	T	C	G
G	G	A	T	C	G	G	C	T	A	G	G	C	T	A
C	C	G	A	T	C	C	T	A	G	C	C	G	A	T
T	T	C	G	A	T	T	A	G	C	T	T	A	G	C
A	A	T	C	G	A	A	G	C	T	A	A	T	C	G

For DNA recovery operations, the corresponding DNA sequences must meet the conditions specified by [36]:

$$\begin{cases} Y_B \neq C_p(Y_B) \neq C_p\big(C_p(Y_B)\big) \neq C_p\big(C_p\big(C_p(Y_B)\big)\big) \\ Y_B = C_p\big(C_p\big(C_p\big(C_p(Y_B)\big)\big)\big) \end{cases}, \tag{2}$$

where Y_B denotes one of the four different basic nucleotides, and $C_p(Y_B)$ is the base pair of Y_B.

2.3. Chaos Theory

Chaos as a nonlinear dynamic process that is highly sensitive to initial states and is unpredictable becomes a natural physical code. It widely applies in the fields of cryptography, random number generation, confidential communication and image encryption. In this paper, two chaos functions containing SLMM and a logistic map are selected to improve the performance of DNA encryption.

2D-SLMM is defined as [48]:

$$\begin{cases} X(n+1) = \alpha(\sin(\pi Y(n)) + \beta)X(n)(1 - X(n)) \\ Y(n+1) = \alpha(\sin(\pi X(n+1)) + \beta)Y(n)(1 - Y(n)) \end{cases}, \tag{3}$$

where α and β are control parameters, and $0 \leq \alpha \leq 1$, $0 \leq \beta \leq 3$. It should be noted that if we want SLMM to work in a chaotic state, the β should close to 3 [48].

There will be a 1D chaos function to describe the logistic map, which is defined as [49]:

$$x(n+1) = \gamma x(n)(1 - x(n)), \tag{4}$$

where $\gamma \in [0, 4]$ is the logistic map parameter, and $x_n \in (0, 1)$. Only when $3.5699456 \leq \gamma \leq 4$, does the logistic map exhibit a state of chaos [49].

2.4. CIIR Algorithm

In the multi-image encryption scheme we proposed, the CIIR algorithm is used to recover different image scenes. However, traditional CIIR algorithms easily cause some pixels to coincide, resulting in a decrease in the intelligibility quality of the recovered scene. To improve the effects of pixel coincidence, we apply a modified reconstruction algorithm [50] so that every reconstructed scene pixel can be calculated. The calculation of the original scene uses the following formula:

$$Y_R(x, y, z) = \frac{1}{T_z} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} E_{i,j}\left(x - i\frac{M \times p}{m \times u}, j\frac{N \times p}{n \times u}\right), \tag{5}$$

where T_z denotes the number of overlaps at the reconstruction distance z, M and N determine the number of EIs, m and n represent the size of the imaging sensor, p represents the pitch between each pinhole, and u is the magnification parameter.

2.5. Entropy Analysis Theory

To illustrate the performance of our proposed encryption scheme quantitatively, we introduce an entropy analysis method. Image entropy describes the average amount of information in an image, representing the aggregation characteristics of the image pixel distribution [51]. For image encryption, the original image contains more spatial features, the pixel distribution is more dispersed, the entropy value is small. While the encrypted image should contain the original image information as less as possible, the pixel distribution is relatively concentrated, so the entropy value is larger than in the original image. Therefore, the size of the entropy value can be analyzed to judge the performance of the encryption scheme.

The entropy of image I can be obtained by the following formula:

$$H(I) = -\sum_{i=1}^{n} P(a_i) \cdot \log_2 P(a_i), \tag{6}$$

where $p(a_i)$ denotes the probability of occurrence of pixel with value of a_i in image I with $0 \le p(a_i) \le 1$ and $\sum_{i=1}^{p}(a_i) = 1$.

3. Multi-Image Encryption Scheme Based on CII

3.1. Framework of Multi-Image Encryption Scheme

In this paper, a multi-image encryption scheme is proposed based the principle of CII, and the overall framework of the scheme is shown in Figure 2.

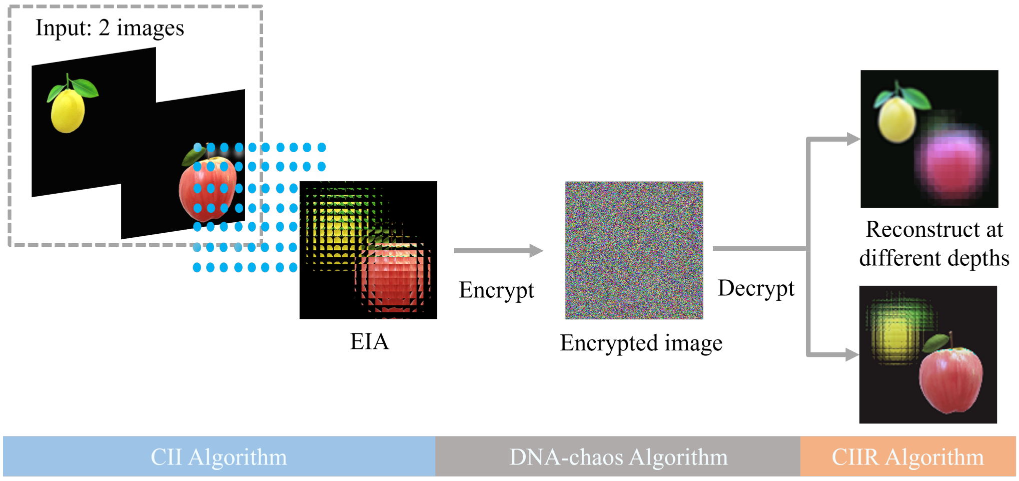

Figure 2. Framework of multi-image encryption scheme.

In the multi-image encryption scheme we proposed, the input can be two or more images (two images are shown in Figure 2, and the following is also described in two images). Firstly, the two input images are placed on different position planes, then it is recorded on an EIA by a microlens array. The EIA merges information from two original images. It is worth noting that the different distances between two images and the microlens array can be used as keys. After that, the EIA is encrypted by the DNA-chaos encryption. Finally, the CIIR is used to reconstruct different original images with different depths. The detailed encryption and decryption procedure is described in Section 3.2.

3.2. Encryption and Decryption Procedure

Figure 3 shows the detailed steps of the encryption algorithm we proposed. It is worth noting that we introduce the chaos algorithm to solve the outline effect caused by the DNA algorithm. The proposed multi-image encryption scheme is a symmetric process, so the decryption process of the image can be achieved by reversing the encryption process. The steps of the decryption process are shown in Figure 4, we only introduce the encryption procedure of the multi-image encryption scheme in detail.

The encryption procedure of the multi-image encryption scheme is introduced as follows:

Step 1 : Convert the original scene into the form of merge image $f(i,j)$ with size $M \times N$ using the integral imaging pickup algorithm.

Step 2: Generate two high-quality pseudo-random sequences $M_1(i,j)$ and $M_2(i,j)$ with size $M \times N$ by cellular automata with two different initial states.

Step 3: Decompose the merge image $f(i,j)$ to three binary matrices $R_1(i,j)$, $G_1(i,j)$ and $B_1(i,j)$ with the size of $M \times N$. Then transform the three binary matrices into three DNA sequence matrices $R_2(i,j)$, $G_2(i,j)$ and $B_2(i,j)$ with the size of $M \times 4N$ based on the DNA coding rules defined in Table 1 and the random encoding sequence $En\_M(i,j)$ generated from pseudo-random sequences $M_1(i,j)$. The random coding sequence $En\_M(i,j)$ can be obtained by:

$$En\_M(i,j) = floor(\text{mod}(M_1(i,j),8)) + 1. \tag{7}$$

Step 4 : Perform the diffusion operations by DNA addition to get three DNA diffused matrices $R_3(i,j)$, $G_3(i,j)$ and $B_3(i,j)$ with the size of $M \times 4N$.

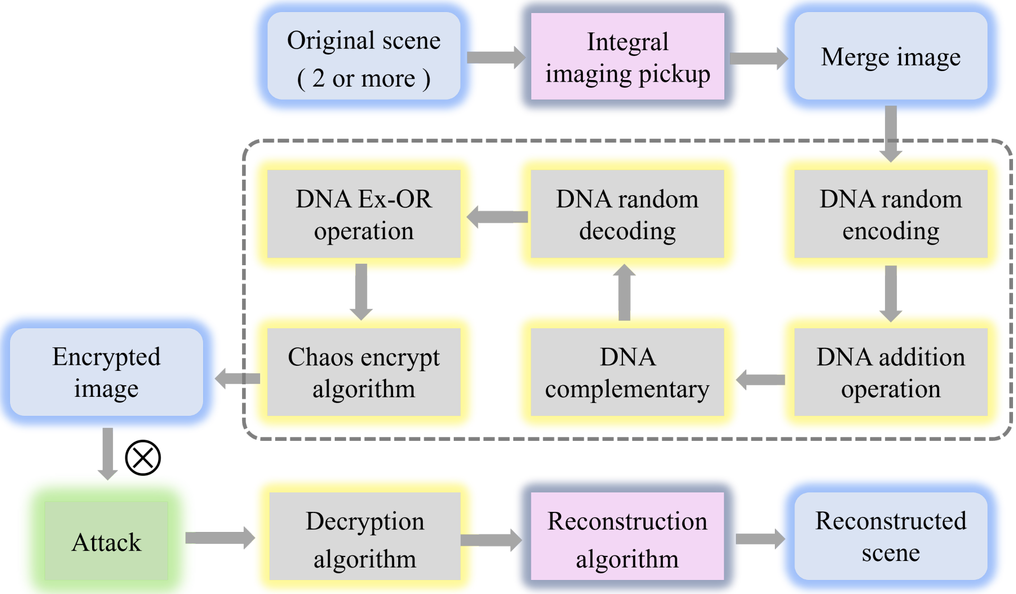

Figure 3. The encryption procedure of multi-image encryption scheme.

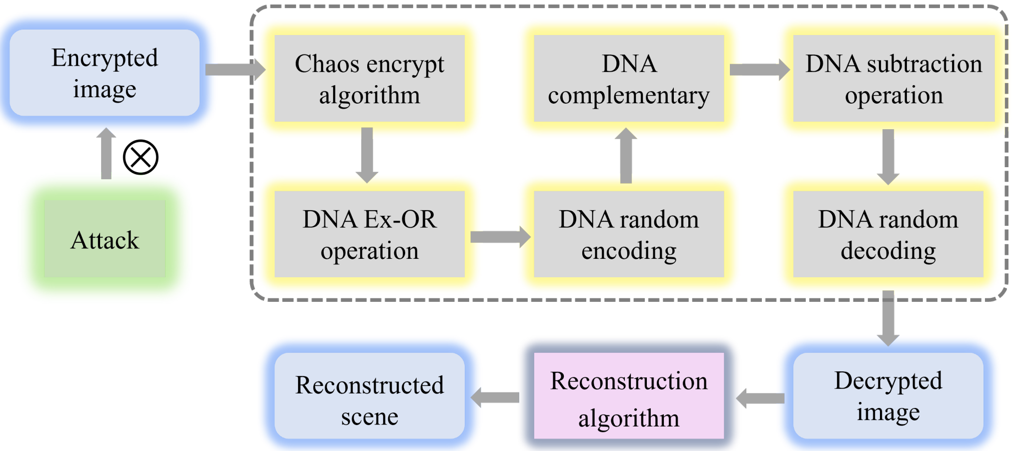

Figure 4. The decryption procedure of multi-image encryption scheme.

Step 5: Select the rule from four complementary rules according to pseudo-random sequence $M_3(i,j)$. Based on $M_3(i,j)$ and the selected complementary rule, perform the DNA complementary operation on DNA diffused matrices and obtain three DNA complementary matrices $R_3'(i,j)$, $G_3'(i,j)$ and $B_3'(i,j)$. The pseudo-random sequence $M_3(i,j)$ is described as:

$$M_3(i,j) = M_1(i,j) \oplus M_2(i,j). \tag{8}$$

Step 6: Decode three DNA matrices $R'_3(i,j)$, $G'_3(i,j)$ and $B'_3(i,j)$ using DNA random decoding sequence $De\_M(i,j)$ generated form pseudo-random sequences $M_2(i,j)$ and the DNA encoding rules. The random decoding sequence is described as:

$$De\_M(i,j) = floor(\bmod(M_2(i,j), 8)) + 1. \tag{9}$$

Step 7: Perform the DNA Ex-OR operations and then convert them into the decimal matrices $R_4(i,j)$, $G_4(i,j)$ and $B_4(i,j)$ with the size of $M \times N$. Perform scrambling operations on the decimal three matrices with three pseudo-random sequences $M_1(i,j)$, $M_2(i,j)$ and $M_3(i,j)$ respectively and obtained decimal three matrices $R_5(i,j)$, $G_5(i,j)$ and $B_5(i,j)$ with the size of $M \times N$.

Step 8: Perform chaos encryption algorithm on the decimal three matrices $R_5(i,j)$, $G_5(i,j)$ and $B_5(i,j)$ and combine them into an encrypted image.

4. Experiment Results and Performance Analysis

In this section, the EIA is calculated by the CII algorithm from two images, "lemon" and "apple". Figure 5 shows the experiment results of the multi-image encryption scheme we proposed. Figure 5a,b shows the original images "lemon" and "apple" with a size of 240 × 240, and Figure 5c shows the EIA of original images "lemon" and "apple" generated by the CII algorithm. Figure 5d shows the encrypted image using the DNA-chaos algorithm. Figure 5e,f shows images reconstructed by the CIIR algorithm, and the reconstruction depths are 15 mm and 6 mm, respectively.

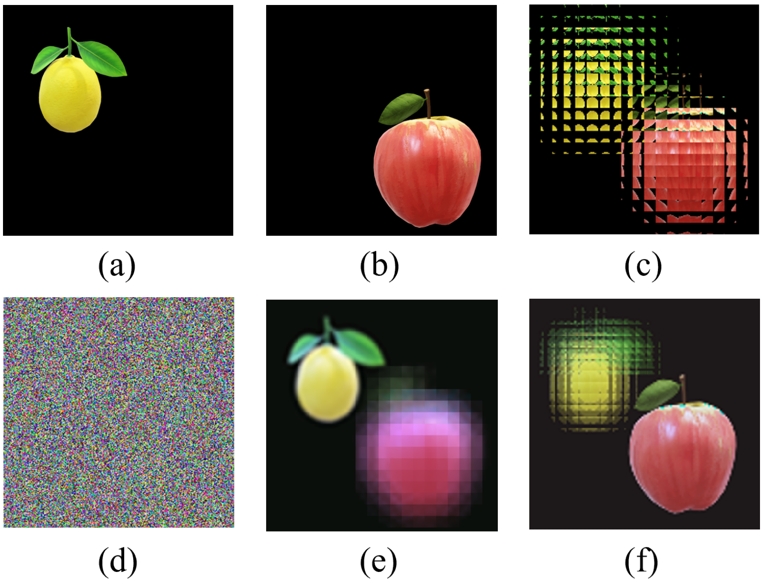

Figure 5. The experiment results of multi-image encryption scheme (240 × 240). (**a**) Original image "lemon". (**b**) Original image "apple". (**c**) EIA of image "lemon" and "apple". (**d**) Encrypted image. (**e**) Reconstructed image (d = 15 mm). (**f**) Reconstructed image (d = 6 mm).

From Figure 5, we can qualitatively see that the multi-image encryption scheme we proposed has an excellent encryption and decryption performance. In order to illustrate that the multi-image encryption scheme we proposed can be applied to different scenarios, we select original images of different sizes and numbers for testing. The experimental results are shown in Figures 6 and 7.

In Figure 6, two original images with a size of 360 × 360 as the encryption images are different from Figure 5 with a size of 240 × 240. From Figure 6, we can also qualitatively see that the multi-image encryption scheme we proposed has an excellent encryption and decryption performance.

In Figure 7, three original images with a size of (240 × 240) are the encryption images. For obvious comparison, we put the encrypted image in the last position. From Figure 7h, we cannot observe any information about the original images. As can be seen from the first three columns in Figure 7, the reconstructed image can clearly restore the information of the original images.

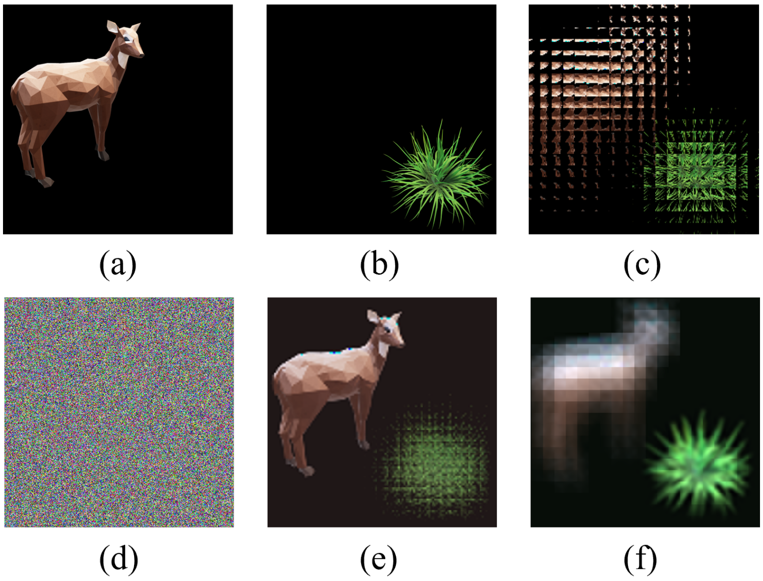

Figure 6. The experiment results of multi-image encryption scheme (360 × 360). (**a**) Original image "sheep". (**b**) Original image "grass". (**c**) EIA of image "sheep" and "grass". (**d**) Encrypted image. (**e**) Reconstructed image (d = 15 mm). (**f**) Reconstructed image (d = 6 mm).

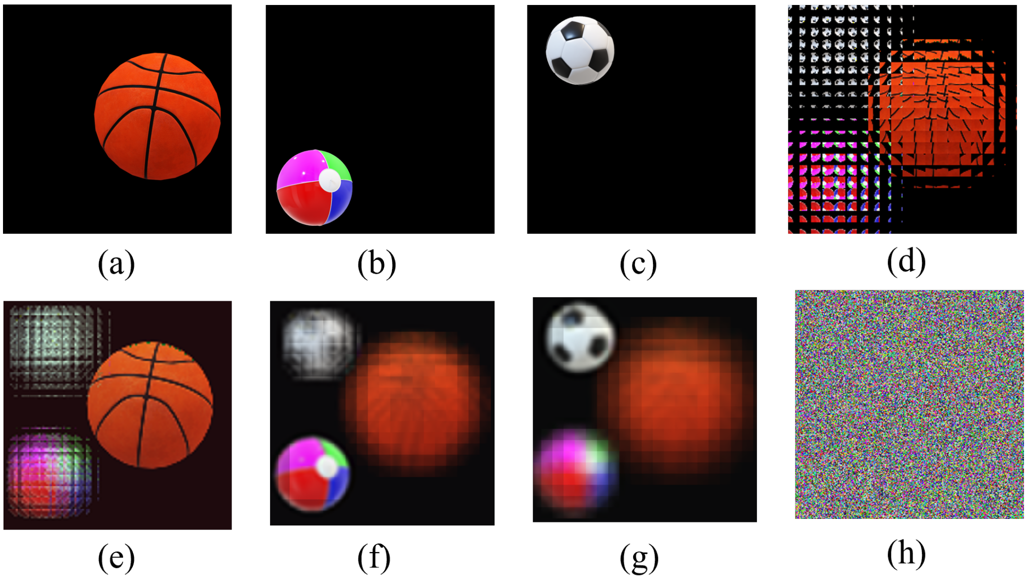

Figure 7. The experiment results with three original images of multi-image encryption scheme (240 × 240). (**a**) Original image "basketball". (**b**) Original image "ball". (**c**) Original image "football". (**d**) EIA of image "basketball", "ball" and "football". (**e**) Reconstructed image (d = 6 mm). (**f**) Reconstructed image (d = 15 mm). (**g**) Reconstructed image (d = 21 mm). (**h**) Encrypted image.

The experimental results in Figures 5–7 fully indicate that the multi-image encryption scheme we proposed can be applied to different scenarios, such as original images of different sizes (240 × 240 in Figure 5 and 360 × 360 in Figure 6) and different numbers (three original images in Figure 7). Following this section, we will analyze the multi-image encryption scheme we proposed quantitatively by taking two original images as examples.

4.1. Key Security Analysis

The encryption scheme must consider the security of the key, that is, the original image cannot be decrypted with the wrong key. Figure 8 shows the results of the key security analysis of our proposed multi-image encryption scheme.

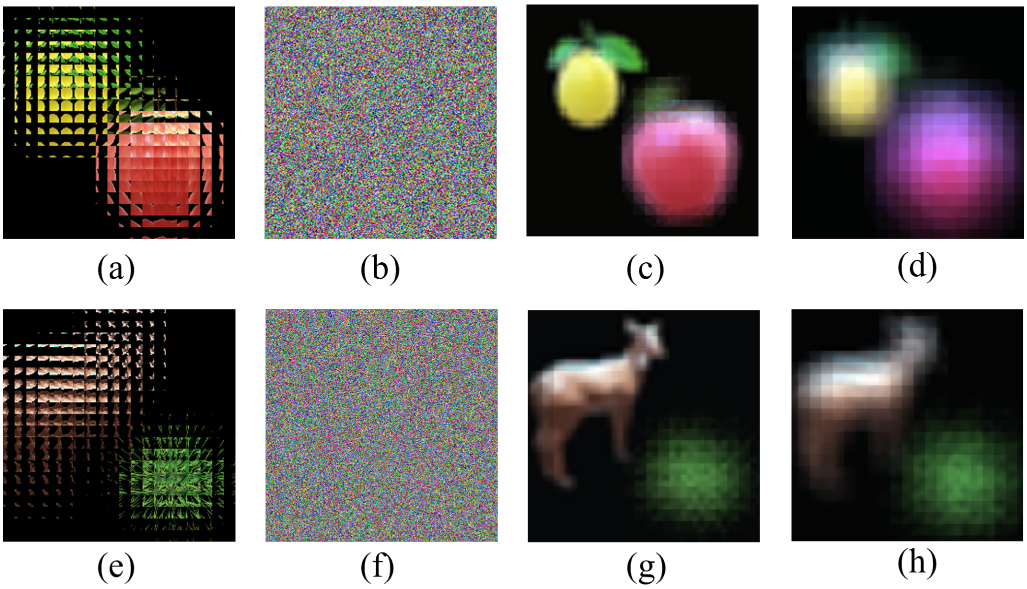

Figure 8. The results of key security analysis. (**a**) The decrypted image of Figure 5d using right key. (**b**) The decrypted image of Figure 5d using wrong key. (**c**) The reconstructed image of Figure 7a with wrong depths (d = 18 mm). (**d**) The reconstructed image of Figure 7a with wrong depths (d = 24 mm). (**e**) The decrypted image of Figure 6d using right key. (**f**) The decrypted image of Figure 6d using wrong key. (**g**) The reconstructed image of Figure 7e with wrong depths (d = 18 mm). (**h**) The reconstructed image of Figure 7e with wrong depths (d = 24 mm).

Figure 8 shows the results of key security analysis; the encrypted images corresponding to the first and second columns are Figures 5d and 6d respectively. Figure 8a,e shows the decrypted image with the right key and Figure 8b,f shows the decrypted image with the wrong key; we cannot obtain any useful information about the original image. Figure 8c,d,g,h separately shows the reconstructed image with wrong depths; when the reconstruction depth is wrong, we cannot obtain a clear image relative to the correct reconstruction depth, such as in Figure 5d,h. This shows that the multi-image encryption scheme we proposed has high key security.

4.2. Statistical Analysis

In order to quantitatively illustrate the performance of our proposed multi-image encryption scheme, we performed a statistical analysis of the experimental results, which is shown in Figure 9.

Figure 9a is the EIA of two original images, "lemon" and "apple", and Figure 9d shows the encrypted image only by DNA algorithm. We can see the outline of two saliency objects in the EIA clearly from the result. Figure 9g represents the image encrypted by the DNA-chaos algorithm, and we cannot see any information about the original image. Figure 9b,e,h represents a histogram (R channel) of Figure 9a,d,g separately. The results of the histogram indicate that the distribution of the image encrypted by DNA-chaos is very flat. Figure 9c,f,i represents the autocorrelation (R channel) of Figure 9a,d,g separately, and we can also find that the autocorrelation is very weak for the image encrypted by DNA-chaos. So the multi-image encryption scheme we proposed has an excellent performance according to the statistical analysis results.

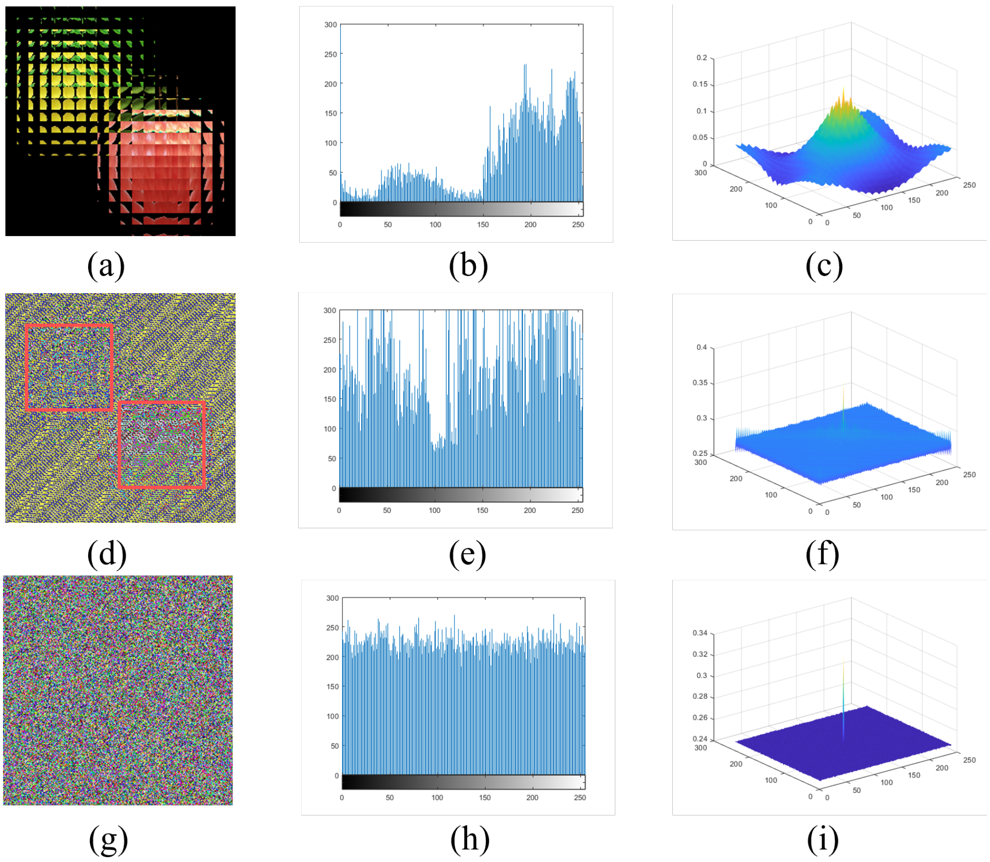

Figure 9. The results of statistical analysis. (**a**) The EIA of two original images. (**d**) The encrypted image only by DNA. (**g**) The encrypted image by DNA-chaos. (**b**,**e**,**h**) represent histogram (R channel) of (**a**,**d**,**g**) respectively. (**c**,**f**,**i**) show autocorrelation results (R channel) of (**a**,**d**,**g**) respectively.

In addition, we calculated the entropy value of Figure 9a,d,g from the RGB channel separately, then took the average of them, and the results are 3.2886, 7.4900 and 7.6277. The entropy value of the encrypted image is significantly larger than the entropy value of the EIA image, which shows that the encryption scheme we proposed performs well.

4.3. Robustness Analysis

In order to verify the reliability of the multi-image encryption scheme we proposed in the noisy environment, we designed simulation experiments to analyze the robustness. We simulated Gaussian noise, Speckle noise, Poisson noise, Salt and Pepper noise and Clip attack channel environments to test the robustness of the scheme. The simulation experiment results are shown in Figure 10.

From Figure 10, we can intuitively see that the multi-image encryption scheme we proposed can reconstruct the original scene correctly in a variety of noise environments.

In order to qualitatively illustrate the visual quality the recovered scene, we use the peak signal-to-noise ratio (PSNR) image quality evaluation index that is widely recognized by researchers. The PSNR value of an image can be obtained by the formula [39]:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE(E, E')}\right), \tag{10}$$

$$MSE = \frac{1}{MN}\sum_{j=0}^{M-1}\sum_{j=0}^{N-1}(E - E')^2, \tag{11}$$

where M and N indicate the width and height of the image, respectively, E is the original scenes, and E' is the recovered scenes.

The PSNR values of the decrypted images with the the Gaussian noise, Speckle noise, Poisson noise, Salt and Pepper noise and Clip attack channel environments are shown in the Table 3.

It can be clearly seen from the Table 3 that the multi-image encryption scheme we proposed has a strong robustness in various noise environments.

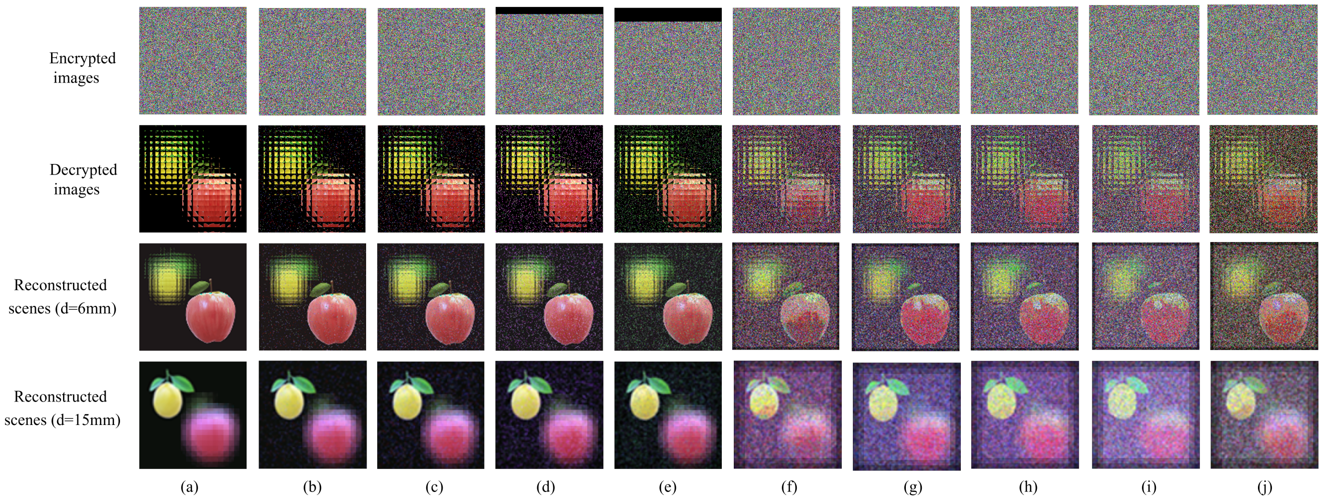

Figure 10. The results of robustness analysis. (**a**) No noise. (**b**) Salt & Pepper noise (0.01). (**c**) Salt & Pepper noise (0.02). (**d**) Clip attack (6.25%). (**e**) Clip attack (12.5%). (**f**) Speckle noise (0.01). (**g**) Speckle noise (0.02). (**h**) Gaussian noise (0.01). (**i**) Gaussian noise (0.02). (**j**) Possion noise.

Table 3. PSNRs of Decrypted Scenes Against Attacks With Different Schemes.

Attacks	R (dB)	G (dB)	B (dB)
Gaussian (0.01)	31.5444	33.0175	34.5347
Gaussian (0.02)	31.3144	32.8944	34.8444
Speckle (0.01)	31.7404	33.2693	34.7687
Speckle (0.02)	31.7186	33.2382	34.4183
Possion	31.7075	33.0537	34.3427
Salt & Pepper (0.01)	43.6942	47.6408	50.1849
Salt & Pepper (0.02)	40.8340	43.9806	46.3331
Clip (6.25 %)	48.6002	43.7822	53.1990
Clip (12.5 %)	38.4986	41.1150	44.3709

There are two indexes to qualitatively illustrate the key sensitivity and plaintext sensitivity encryption scheme, namely number of pixels change rate (NPCR) and unified average changing intensity (UACI) [52]. NPCR indicates the number of pixels that change between two images and UACI represents the average number of changes in intensity between two images. The calculation formula of NPCR and UACI is as follows:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{12}$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100, \% \tag{13}$$

where $D(i, j)$ is defined as:

$$D(i, j) = \begin{cases} 1, C_1(i, j) \neq C_2(i, j) \\ 0, \text{ otherwise,} \end{cases} \tag{14}$$

where W and H denote the width and height of the image. $C1$ and $C2$ are two images.

That the plaintext images are sensitive is a basic requirement of a good image cryptosystem. Only those image cryptosystems with plaintext sensitivity can resist the chosen/known plaintext attacks. For any given key, if the plain image is changed slightly, its encrypted image will be changed dramatically, and this image cryptosystem is plaintext sensitive.

Key sensitivity analysis includes three aspects: (1) When encrypting a plaintext image, if the key changes slightly, the encryption system will produce two completely different encrypted images, which means that the key is sensitive in the encryption process. Meanwhile, such a key is an effective encryption key; (2) When encrypting a plaintext image, if the key changes slightly, the encryption system will produce two completely different encrypted images, which means that the key is sensitive in the encryption process. Meanwhile, such a key is an effective encryption key; (3) When decrypting a cipher image using an illegal key, if the key changes slightly, the decryption system will produce two completely different images, both totally different from the original plaintext image. This means that the illegal key is sensitive in the decryption process. Such an illegal key is effective.

We use NPCR and UACI to qualitatively illustrate the key sensitivity and plaintext sensitivity of the multi-image encryption scheme we proposed. We still use Figure 5c as our test image; the results are shown in Table 4.

Table 4. The analysis of key sensitivity and plaintext sensitivity using NPCR and UACI.

Index	NPCR (%)	UACI (%)
Plaintext sensitivity	99.6091	33.4591
Encryption process	99.6100	33.4603
Decryption process (legal)	99.6064	28.6356
Decryption process (illegal)	99.6085	33.4673
Theoretical value	**99.6094**	**33.4635**

The theoretical value of NPCR is 99.6094% and UACI is 33.4635%. From the Table 4, we can find that the NPCR and UACI are very close to the theoretical value, Which indicates the multi-image encryption scheme we proposed has excellent key sensitivity and plaintext sensitivity.

4.4. Time Analysis

Encryption time is very important for an encryption scheme. An image encryption scheme with good performance should use as little time as possible in the process of image encryption and decryption. In this section, we select different sizes of images and more than two images as input to test the multi-image encryption scheme we proposed. The results of the encryption and decryption analysis of different images are shown in Figure 11.

Figure 11a is the EIA of two input images with the size of 240 × 240, Figure 11d is the EIA of two input images with the size of 360 × 360, and Figure 11g is the EIA of three input images with the size of 240 × 240. We analysis the encryption and decryption time of these different images. For Figure 11a, the encryption and decryption time is 3.1225 s, Figure 11d is 4.3257 s and Figure 11d is 4.6328 s.

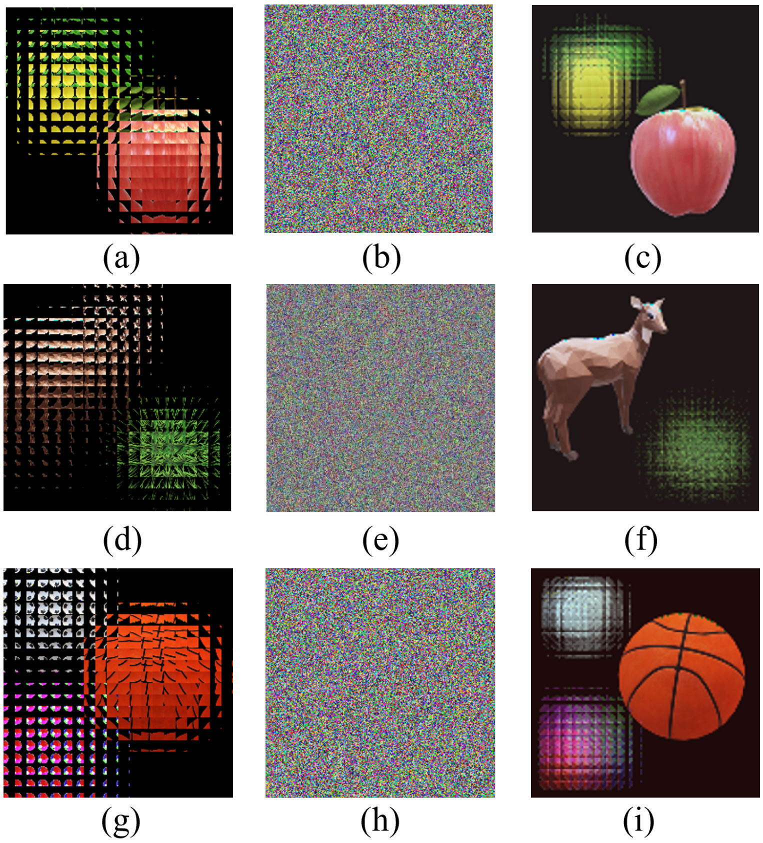

Figure 11. Encryption and decryption analysis of different images. (**a**) The EIA of two input images (240 × 240). (**d**) The EIA of two input images (360 × 360). (**g**) The EIA of three input images (240 × 240). (**b**,**e**,**h**) represent encrypted image of (**a**,**d**,**g**) separately. (**c**,**f**,**i**) show decryption results of (**a**,**d**,**g**) separately.

5. Conclusions

In conclusion, we apply the CII algorithm to achieve multi-image encryption, which significantly improves the efficiency of image encryption, meanwhile combining the chaos algorithm to address the outline effect caused by the DNA encryption algorithm. In the proposed multi-image encryption scheme, the different depth distances of multiple images can also be used as keys, which can improve the security of the encryption method significantly. We also analyze the robustness of this scheme against a variety of attacks. The experiment results confirm the excellent performance of our proposed multi-image encryption scheme.

Author Contributions: Conceptualization, X.L., C.Y. and J.G.; methodology, X.L. and J.G.; formal analysis, X.L. and J.G.; writing—original draft preparation, X.L. and J.G.; writing—review and editing, C.Y. and J.G. All the authors made comments on the final version before the submission. All authors have read and agreed to the published version of the manuscript.

Funding: Natural Science Foundation of Guangdong Province (2018A0303070009, 2021A1515011091); Educational Commission of Guangdong Province (2018KTSCX143, 2020ZDZX3056).

Data Availability Statement: Not applicable.

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

References

1. Chen, W.; Javidi, B.; Chen, X. Advances in optical security systems. *Adv. Opt. Photonics* **2014**, *6*, 120–155. [CrossRef]
2. Wang, X.; Zhu, X.; Wu, X.; Zhang, Y. Image encryption algorithm based on multiple mixed hash functions and cyclic shift. *Opt. Lasers Eng.* **2018**, *107*, 370–379. [CrossRef]

3. Shi, Y.; Li, T.; Wang, Y.; Gao, Q.; Zhang, S.; Li, H. Optical image encryption via ptychography. *Opt. Lett.* **2013** , *38* , 1425–1427. [CrossRef] [PubMed]
4. Li, X.; Meng, X.; Yang, X., Yin; Y.; Wang, Y.; Peng, X.; Chen, H. Multiple-image encryption based on compressive ghost imaging and coordinate sampling. *IEEE Photonics J.* **2016**, *8*, 1–11.
5. Li, X.; Xiao, D.; Wang, Q.H. Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. *Opt. Lasers Eng.* **2018**, *100*, 200–207. [CrossRef]
6. Zhao, R.; Zhang, Y.; Xiao, X.; Ye, X.; Lan, R. TPE2: Three-pixel exact thumbnail-preserving image encryption. *Signal Process.* **2021**, *183*, 108019. [CrossRef]
7. Gong, L.; Qiu, K.; Deng, C.; Zhou, N. An optical image compression and encryption scheme based on compressive sensing and RSA algorithm. *Opt. Lasers Eng.* **2019**, *121*, 169–180. [CrossRef]
8. Qu, G.; Yang, W.; Song, Q.; Liu, Y.; Qiu, C.W.; Han, J.; Xiao, S. Reprogrammable metahologram for optical encryption. *Nat. Commun.* **2014**, *11*, 5484.
9. Pan, A.; Wen, K.; Yao, B. Linear space-variant optical cryptosystem via Fourier ptychography. *Opt. Lett.* **2019**, *44*, 2032–2035. [CrossRef]
10. Chen, W.; Situ, G.; Chen, X. High-flexibility optical encryption via aperture movement. *Opt. Express* **2013**, *21*, 24680–24691. [CrossRef]
11. Liu, Z.; Xu, L.; Lin, C.; Liu, S. Image encryption by encoding with a nonuniform optical beam in gyrator transform domains. *Appl. Opt.* **2010**, *49*, 563–5637. [CrossRef]
12. Yang, B.; Liu, Z.; Wang, B.; Zhang, Y.; Liu, S. Optical stream-cipher-like system for image encryption based on Michelson interferometer. *Opt. Express* **2011**, *19*, 2634–2642. [CrossRef]
13. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
14. Peng, X.; Zhang, P.; Wei, H.; Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **2006**, *31*, 1044–1046. [CrossRef]
15. Unnikrishnan G.; Joseph J.; Singh K. Optical Encryption by Double-random Phase Encoding in the Fractional Fourier Domain *Opt. Lett.* **2000**, *25*, 887–889. [CrossRef]
16. Situ, G.H.; Zhang, J. Double random-phase encoding in the Fresnel domain. *Opt. Lett.* **2014**, *29*, 1584–1586. [CrossRef]
17. Liu, Z.J.; Xu, L.; Lin, C. Image encryption scheme by using iterative random phase encoding in gyrator transform domains. *Opt. Lasers Eng.* **2011**, *49*, 542–546. [CrossRef]
18. Kumar, R.; Bhaduri, B. Optical image encryption in Fresnel domain using spiral phase transform. *J. Opt.* **2017**, *19*, 095771. [CrossRef]
19. Sui, L.S.; Xu, M.J.; Tian, A.L. Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain. *Opt. Lasers Eng.* **2017**, *91*, 106–114. [CrossRef]
20. Zhao, D.M.; Li, X.; Chen, L.F. Optical image encryption with redefined fractional Hartley transform. *Opt. Commun.* **2008**, *281*, 5326–5329. [CrossRef]
21. Hong, S.H.; Jang, J.S.; Javidi, B. Three-dimensional volumetric object reconstruction using computational integral imaging. *Opt. Express* **2004**, *12*, 483–491. [CrossRef] [PubMed]
22. Shin, D.H.; Yoo, H. Image quality enhancement in 3D computational integral imaging by use of interpolation methods. *Opt. Express* **2007**, *15*, 12039–12049. [CrossRef]
23. Chen, Y.; Wang, X.; Zhang, J.; Yu, S.; Zhang, Q.; Guo, B. Resolution improvement of integral imaging based on time multiplexing sub-pixel coding method on common display panel. *Opt. Express* **2014**, *22*, 17897–17907. [CrossRef]
24. Wang, Y.J.; Shen, X.; Lin, Y.H.; Javidi, B. Extended depth-of-field 3D endoscopy with synthetic aperture integral imaging using an electrically tunable focal-length liquid-crystal lens. *Opt. Lett.* **2015**, *40*, 3564–3567. [CrossRef]
25. Stern, A.; Javidi, B. Three-dimensional image sensing and reconstruction with time-division multiplexed computational integral imaging. *Appl. Opt.* **2003**, *42*, 7036–7042. [CrossRef]
26. Adleman, L.M. Molecular computation of solutions to combinatorial problems. *Science* **1994**, *266*, 1021–1024. [CrossRef]
27. Xiao, X.; Javidi, B. Martinez-Corral, M.; Stern, A. Advances in three-dimensional integral imaging: Sensing, display, and applications. *Appl. Opt.* **2013**, *52*, 546–560. [CrossRef]
28. Li, X.; Zhao, M.; Xing, Y.; Zhang, H.L.; Li, L.; Kim, S.T.; Wang, Q.H. Designing optical 3D images encryption and reconstruction using monospectral synthetic aperture integral imaging. *Optics Express* **2018**, *26*, 11084–11099. [CrossRef]
29. Li, X.; Zhao, M.; Xing, Y.; Li, L.; Kim, S.T.; Zhou, X.; Wang, Q.H. Optical encryption via monospectral integral imaging. *Opt. Express* **2017**, *25*, 31516–31527. [CrossRef]
30. Markman, A.; Wang, J.; Javidi, B. Three-dimensional integral imaging displays using a quick-response encoded elemental image array. *Optica* **2014**, *1*, 332–335. [CrossRef]
31. Park, G.; Jung, J.H.; Hong, K.; Kim, Y.; Kim, Y.H.; Min, S.W.; Lee, B. Multi-viewer tracking integral imaging system and its viewing zone analysis. *Opt. Express* **2009**, *17*, 17895–17908. [CrossRef] [PubMed]
32. Xing, S.; Sang, X.; Yu, X.; Duo, C.; Pang, B.; Gao, X.; Wang, K. High-efficient computer-generated integral imaging based on the backward ray-tracing technique and optical reconstruction. *Opt. Express* **2017**, *25*, 330–338. [CrossRef] [PubMed]

33. Wang, Y.; Ren, Z.; Zhang, L.; Li, D.,; Li, X. 3D image hiding using deep demosaicking and computational integral imaging. *Opt. Lasers Eng.* **2022**, *148*, 106772. [CrossRef]
34. Watson, J. D.; Crick, F.H. Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid. *Nature* **1953**, *171*, 737–738. [CrossRef]
35. Sun, S. A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. *IEEE Photonics J.* **2018**, *10*, 1–14. [CrossRef]
36. Liu, H.; Wang, X. Image encryption using DNA complementary rule and chaotic maps. *Appl. Soft Comput.* **2012**, *12*, 1457–1466. [CrossRef]
37. Guesmi, R.; Farah, M.A.B.; Kachouri, A.; Samet, M. A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. *Nonlinear Dyn.* **2016**, *83*, 1123–1136. [CrossRef]
38. Fu, X.Q.; Liu, B.C.; Xie, Y.Y.; Li, W.; Liu, Y. Image encryption-then-transmission using DNA encryption algorithm and the double chaos. *IEEE Photonics J.* **2018**, *10*, 1–15. [CrossRef]
39. Wang, Y.; Li, X. W.; Wang, Q.H. Integral imaging based optical image encryption using CA-DNA algorithm. *IEEE Photonics J.* **2021**, *13*, 1–12. [CrossRef]
40. Zhang, Y.Q.; Wang, X.Y.; Liu, J.; Chi, Z.L. An image encryption scheme based on the MLNCML system using DNA sequences. *Adv. Opt. Photonics* **2016**, *82*, 95–103. [CrossRef]
41. Zhang, Y.; Wang, P.; Huang, H.; Zhu, Y.; Xiao, D.; Xiang, Y. Privacy-assured FogCS: Chaotic compressive sensing for secure industrial big image data processing in fog computing. *IEEE Trans. Ind. Inform.* **2020**, *17*, 3401–3411. [CrossRef]
42. Head, T.; Rozenberg, G.; Bladergroen, R.S.; Breek, C.K.D.; Lommerse, P.H.M.; Spaink, H.P. Computing with DNA by operating on plasmids. *BioSystems* **2000**, *57*, 87–93. [CrossRef]
43. Zheng, X.; Xu, J.; Li, W. Parallel DNA arithmetic operation based on n-moduli set. *Appl. Math. Comput.* **2015**, *297*, 80–94. [CrossRef]
44. Hayat, U.; Azam, N.A. A novel image encryption scheme based on an elliptic curve. *Signal Process.* **2019**, *155*, 391–402. [CrossRef]
45. Azam, N.A.; Ullah, I.; Hayat, U. A fast and secure public-key image encryption scheme based on Mordell elliptic curves. *Opt. Lasers Eng.* **2021**, *137*, 106371. [CrossRef]
46. Jia, N.; Liu, S.; Ding, Q.; Wu, S.; Pan, X. A New Method of Encryption Algorithm Based on Chaos and ECC. *J. Inf. Hiding Multim. Signal Process.* **2016**, *7*, 637–644.
47. Zhang, F.; Zhang, Z.; Guan, P. ECC2: Error correcting code and elliptic curve based cryptosystem. *Inf. Sci.* **2020**, *526*, 301–320. [CrossRef]
48. Hua, Z.Y.; Zhou, Y.C.; Pun, C.M.; Chen, C.L.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2014**, *6*, 120–155. [CrossRef]
49. Singh, N.; Sinha, A. Optical image encryption using Hartley transform and logistic map. *Opt. Commun.* **2009**, *282*, 1104–1109. [CrossRef]
50. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **2017**, *90*, 225–237. [CrossRef]
51. Tsai, D.Y.; Lee, Y.; Matsuyama, E. Information entropy measure for evaluation of image quality. *J Digit Imaging* **2008**, *21*, 338–347. [CrossRef] [PubMed]
52. Chai, X.; Gan, Z.; Yuan, K.; Chen, Y.; Liu, X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural. Comput. Appl.* **2019**, *31*, 219–237. [CrossRef]