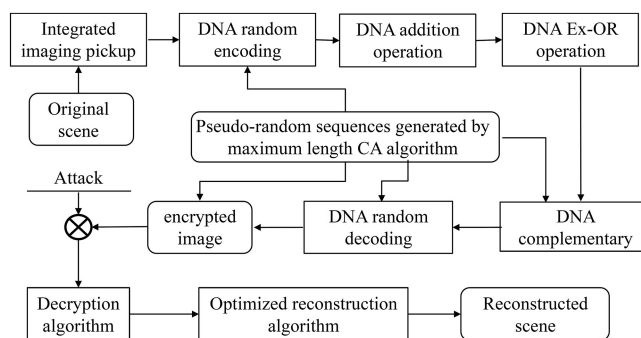


Integral Imaging Based Optical Image Encryption Using CA-DNA Algorithm


Volume 13, Number 2, April 2021

Ying Wang
Xiao-Wei Li
Qiong-Hua Wang



DOI: 10.1109/JPHOT.2021.3068161

Integral Imaging Based Optical Image Encryption Using CA-DNA Algorithm

Ying Wang,¹ Xiao-Wei Li,¹ and Qiong-Hua Wang ²

¹School of Electronics and Information Engineering, Sichuan University, Chengdu 610065, China

²School of Instrumentation and Optoelectronic Engineering, Beihang University, Beijing 100191, China

DOI:10.1109/JPHOT.2021.3068161

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see <https://creativecommons.org/licenses/by/4.0/>

Manuscript received November 24, 2020; revised March 10, 2021; accepted March 19, 2021. Date of publication March 23, 2021; date of current version April 9, 2021. This research was supported by the Program for National Natural Science Foundation of China (NSFC) under Grant 61975138. Corresponding author: Qiong-Hua Wang (e-mail: qionghua@buaa.edu.cn).

Abstract: Under the computational integral imaging-based security system, the application of Deoxyribonucleic Acid (DNA) encoding algorithm will cause silhouettes in the cipher image, thereby reducing the security of the system. To solve this problem, we introduced a cellular automata-based DNA (CA-DNA) algorithm, which effectively hides the distribution information of the original scene. It can prevent attackers from obtaining any valid information based on the statistical characteristics of the image, which makes our encryption system more security. At the same time, an improved high-resolution reconstruction algorithm is applied to achieve a high-quality decrypted scene. We conducted relevant experiments to certificate the effectiveness of proposed method. Experimental results verify that the scheme has high security and robustness.

Index Terms: Optical encryption algorithm, Deoxyribonucleic Acid algorithm, cellular automata, computational integral imaging.

1. Introduction

In the Internet era, massive multi-dimensional image data are transmitted on the network every moment. To protect the privacy of the authorized users, information protection has become a key task in image transmission. The cryptosystem is an effective means to ensure information security [1]–[5]. Among them, the optical encryption method is widely applied in the field of image encryption due to its significant advantages. It has become a major topic in the research of image security. There are many optical technologies used in image protection, and then a variety of optical image encryption algorithms have been proposed [6]–[11]. As an excellent optical imaging system, computational integral imaging (CII) can display full-color images with a wide field of view and continuous parallax [12]–[18]. Because this algorithm can record scenes into a hologram-like characteristic element image array (EIA) [18]–[22], it has attracted attention in the field of optical data security. Some cryptosystems based on the CII framework have been proposed [23]–[26]. These algorithms have significant advantages of high processing speed and high robustness.

Recently, due to the advantages of the parallelism and high information density of deoxyribonucleic acid (DNA) algorithm, some DNA-based encryption methods have been proposed [27]–[28]. Relevant researches have proved that DNA coding technology can effectively resist chosen plaintext attacks, thereby improving the security of cryptosystems [29]–[31]. Many image encryption

methods that combine DNA coding with chaos have been proposed [32]–[33]. DNA sequence operations and Logistic mapping are used in image encryption algorithms. In addition, in order to overcome the security shortcomings of low-dimensional chaotic systems, hyperchaotic systems are used for image encryption [34]–[37]. Most conventional DNA coding-based encryption schemes use fixed coding rules, which has the advantages of being easy to implement and having a low time load. However, for some special images, such as element images, fixed DNA coding rules cannot change the bit distribution of these images. Therefore, it leads to contour problems in the cipher-text. It will reveal the distribution information of the original scene and provide potential clues for attackers to establish a cryptographic system.

To overcome this problem, we introduced the cellular automata (CA) algorithm. CA is a dynamic system based on a finite state set [38]–[40]. The CA-based encryption method is a natural choice for secure transmission and has significant advantages [41]–[43]. In the case of large-scale parallel computing, CA can calculate pseudo-random numbers in parallel, which is of great significance in image encryption. Moreover, benefiting from the mathematical characteristics of CA, compared with the existing algorithms, it can provide a significant advantage algorithm [44]–[46]. The CA encoding algorithm has a large key space because its neighbor size, rules, maximum state, and the initial values can all be used as key parameters for the encryption system. Meanwhile, the complexity of CA makes it difficult for CA-based encryption system to be attacked.

In this paper we propose a high security optical encryption approach based on computational integral imaging and CA-based DNA (CA-DNA) encryption algorithm. The high-quality random sequences generated by the CA algorithm are used to define which encoding or decoding rules are applied to each pixel of the EIA. Therefore, in our algorithm not all pixel coding rules are fixed, which better hides the distribution information of element images. The attacker cannot obtain any valid information based on the statistical distribution of the images, which makes the encryption system more secure. And the CA-DNA complementary operation is applied to further improve the security of the system. In other words, it provides a high-security encryption scheme. Furthermore, a modified computational integral imaging reconstruction algorithm is applied to improve the view quality of the decrypted scene. To prove the feasibility and security of the encoding approach, numerical experiments are conducted, and the results are discussed.

2. Theoretical Analysis of the Proposed Method

2.1. EIA Captured by the Integral Imaging System

CII [13] algorithm is an important part of the imaging system, which plays an important role in 3D image processing. Because of its high security and flexibility, it has received attention in the field of information security. It contains two parts, one of which is the process of picking up the original scene, and the other part is the process of EIA reconstruction.

Fig. 1 demonstrate the process of picking up the original scene. Through the lenslet array and image sensor, the original scene to be encrypted is converted to EIs. The (i, j) th elemental image can be obtained by the formula[13]:

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

where x and y denote the lenslet array coordinates, ϕ is the size of each lens, and z is the distance between the original scene and the lenslet array.

2.2. DNA Sequence Operations

DNA sequence contains four kinds of nucleic acid bases, namely adenine (A), thymine (T), cytosine (C) and guanine (G). If they are defined as numbers “00”, “11”, “01” and “10”, then the digital image can be represented as a corresponding nucleotide string. Among all the 24 types of DNA coding rules, only eight types meet the Watson-Crick complementarity rule. They are recorded in Table 1

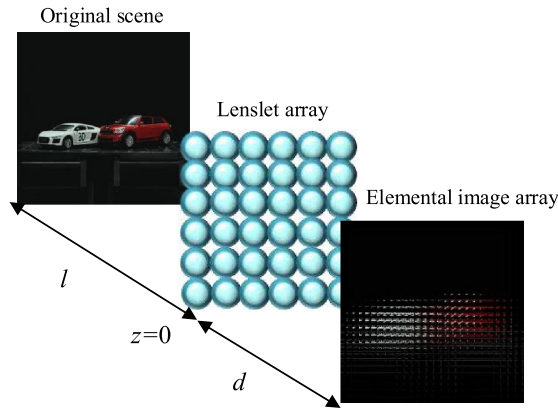


Fig. 1. The pickup process of the integral imaging system.

TABLE 1
DNA Coding Rules

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

TABLE 2
DNA Addition, Subtraction, and Ex-OR 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	G	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	C	A	A	G	C	T	A	A	T	C	G

[27]. During the encryption process, we will select these encoding rules through CA sequence to randomly encode each pixel.

In the DNA method, there are addition, subtraction, and exclusive-OR (Ex-OR) operations. The calculation rules of these operations depend on the corresponding DNA coding rules. Table 2 shows the corresponding addition, subtraction, and Ex-OR operations when the DNA coding rule is one [27]. Therefore, for DNA-level images, these three DNA operations can be utilized to scramble adjacent bases, or adjacent DNA sequences.

Moreover, for DNA complementation operation, the complementary rules between four DNA bases must satisfy the following conditions [29]:

$$\begin{cases} Y_B \neq F_p(Y_B) \neq F_p(F_p(Y_B)) \neq F_p(F_p(F_p(Y_B))), \\ Y_B = F_p(F_p(F_p(Y_B))), \end{cases} \quad (2)$$

where $F_p(Y_B)$ is the base pair of Y_B . Each base of the DNA sequence has six main complementary rules. In this method, one of the six complementary rules are selected to complement the diffusion

process through the CA random sequence of each DNA sequence, thereby improving encryption efficiency.

2.3. High-Quality Pseudo-Random Sequence Generated by CA Algorithm

The core of the CA algorithm is a discrete dynamic model composed of the arrangement and rules of cells. Benefiting from the mathematical characteristics of the CA algorithm, it can provide significant advantages compared to the existing algorithms. The CA algorithm has a large key space, because its neighbor size, rules, maximum state, and initial values can all be used as the key parameters of the cryptosystem. Moreover, the keys of the CA encoding system can select a generating function with an avalanche effect. For the same image, a small change in the CA key will result in a great change in the pixel distribution of the cryptographic image. And a tiny change in the original image using the same key will also greatly affect the information distribution of the cipher image. The complexity of CA algorithm makes the CA-based encryption system difficult to be attacked. For a one-dimension (1D) CA with two states and three sites neighborhoods, the update of the next state of each unit depends on the state of its neighborhood. The value of each unit is calculated by a prescribed rule. Through the Boolean function can calculate the value of the next state:

$$c_m(k+1) = F_B(c_{m-1}(k), c_m(k), c_{m+1}(k)), \quad (3)$$

where $F_B()$ denotes the Boolean function with defined rules, $c_m(k)$, $c_{m-1}(k)$, and $c_{m+1}(k)$ represent the states of m -th cell and its neighbors at time k , respectively. According to Wolfram's theory, a CA with two states and three sites has 28 types of Wolfram rules [38], whose range is defined as 0 to 255. Among these Wolfram rules, only eight types of rules are linear. However, rules 0, 60, 102, 170, 204, and 240 cannot generate random sequences that meet the cryptography requirements. By combining rules 90 and 150, the efficient maximum length random sequence can be generated. The calculated high-quality random sequence will be utilized to encrypt the plaintext. The equations of rules 90 and 150 are written as:

$$\begin{aligned} \text{rule 90 : } c_m(k+1) &= c_{m-1}(k) \oplus c_{m+1}(k), \\ \text{rule 150 : } c_m(k+1) &= c_{m-1}(k) \oplus c_m(k) \oplus c_{m+1}(k), \end{aligned} \quad (4)$$

and the corresponding characteristic polynomial is:

$$y(c) = c^8 + c^7 + c^5 + c^3 + 1. \quad (5)$$

2.4. Modified Computational Integral Imaging Reconstruction Algorithm

The 3D scene can be recovered by a computational reconstruction algorithm. According to the principle of geometrical optics [22], [23], each elemental image is inversely mapped according to the magnification factor. However, with the computational integral imaging reconstruction (CIIR) scheme, the superposition of the pixels will reduce the quality of the recovered scene. Fig. 2 shows that the superposition process of the 3D scene reconstruction.

In order to mitigate the effect of fuzzy noise caused by the pixel's superposition, we applied a modified reconstruction algorithm [39]. Each pixel in the recovered scene can be calculated, and the following formula can be utilized to reconstruct the original scene:

$$Y_R(x, y, z) = \frac{1}{T_z} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} E_{i,j} \left(x - i \frac{M \times p}{m \times u}, j \frac{N \times p}{n \times u} \right), \quad (6)$$

where T_z is the superimposed matrix at the distance z , $M \times N$ represents the numbers of element images, m and n are the size of the imaging device, p denotes the size of the pinhole, and u denotes the magnification parameter.

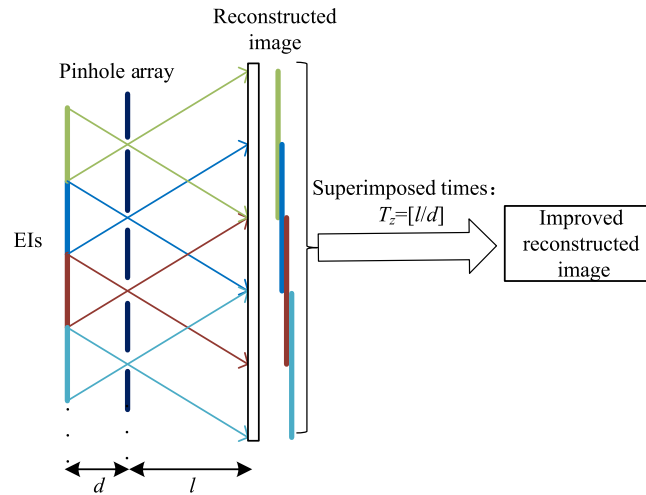


Fig. 2. Modified computational integral imaging reconstruction algorithm.

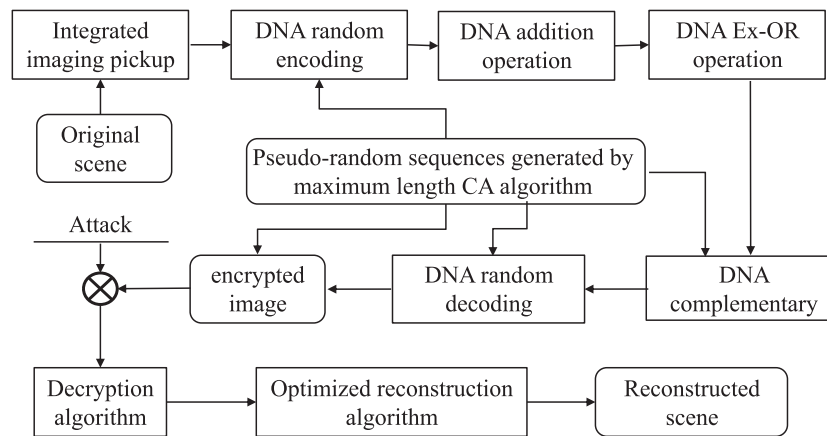


Fig. 3. Flow chart of the proposed encryption scheme.

3. Description of the Encryption and Decryption Procedure

In the previous DNA-based encryption system, the generated element image can be scrambled using the DNA encoding method. However, the pixel values of the element image have not been changed, which leads to silhouette problems in the encrypted image. It makes the encryption system vulnerable to statistical attacks. A CA-DNA encryption approach can change pixel values of element image and provide a cipher-text with uniform information distribution. Fig. 3 describes the flow chart of our encryption algorithm. The encryption procedure of our scheme is introduced as follows:

Step 1: Convert the original 3D scene into the form of 2D elemental image $f(i, j)$ with size $M \times N$ using the CII 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 two different groups CA rules.

Step 3: Decompose the EIA $f(i, j)$ 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 size $M \times 4N$ based on the DNA coding rules defined in Table 1 and the

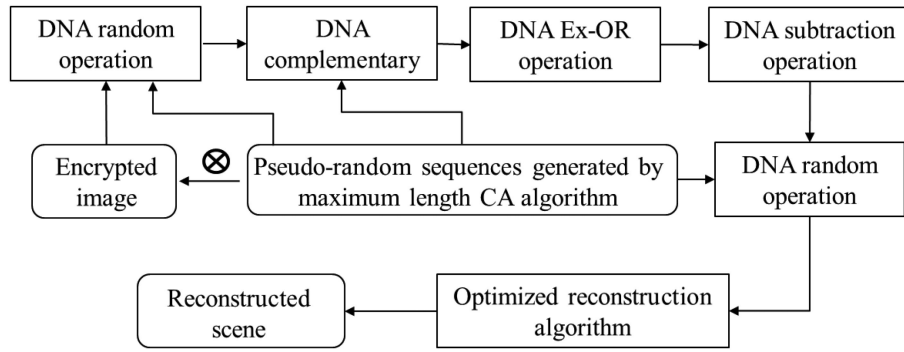


Fig. 4. Decryption process of the proposed scheme.

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:

$$En_M(i, j) = \text{floor}(\text{mod}(M_1(i, j), 8)) + 1. \quad (7)$$

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

Step 5: Select the rule from six complementary rules according pseudo-random sequence $M_3(i, j)$. Based on $M_3(i, j)$ and selected complementary rule, perform 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:

$$M_3(i, j) = M_1(i, j) \oplus M_2(i, j). \quad (8)$$

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 from pseudo-random sequences $M_2(i, j)$ and the DNA encoding rules, then convert them into the decimal matrices $R_4(i, j)$, $G_4(i, j)$, and $B_4(i, j)$. The random decoding sequence is described as:

$$De_M(i, j) = \text{floor}(\text{mod}(M_2(i, j), 8)) + 1. \quad (9)$$

Step 7: Perform scrambling operations on the decimal three matrices $R_4(i, j)$, $G_4(i, j)$, and $B_4(i, j)$ with three pseudo-random sequences $M_1(i, j)$, $M_2(i, j)$, and $M_3(i, j)$ respectively, and combine them into a cipher image.

The proposed scheme is a symmetric encryption system, so the image can be decrypted by the reverse operation of the encryption process. The decryption process is shown in Fig. 4.

4. Experimental Results

In this section, we confirm the capability of the proposed scheme through a series of simulation experiments. The EIA is generated from the original scene "Cars" by the CII algorithm. For encryption system, we use two sets of linear CA rules (rules (150; 150; 90; 150; 90; 150; 90; 150) and rules (150; 90; 150; 90; 90; 90; 150; 90)) to generate two high-quality random sequences. Fig. 5(a) shows the recorded original elemental image of "Cars" with the size of 355×355 , and Fig. 5(b) is the encrypted image obtained by the proposed optical encryption algorithm. Figs 5(c)-5(e) show the recovered scenes obtained using a modified computational integral imaging reconstruction algorithm at different depths, and Fig. 5(f) illustrates the recovered scene obtained at the correct depth (100mm) using the CIIR algorithm. Since the encryption process includes seven steps, the time complexity of the proposed algorithm is determined by all the steps of the encryption algorithm, so the total time complexity of the proposed scheme is $O(24 \times M \times N)$. And

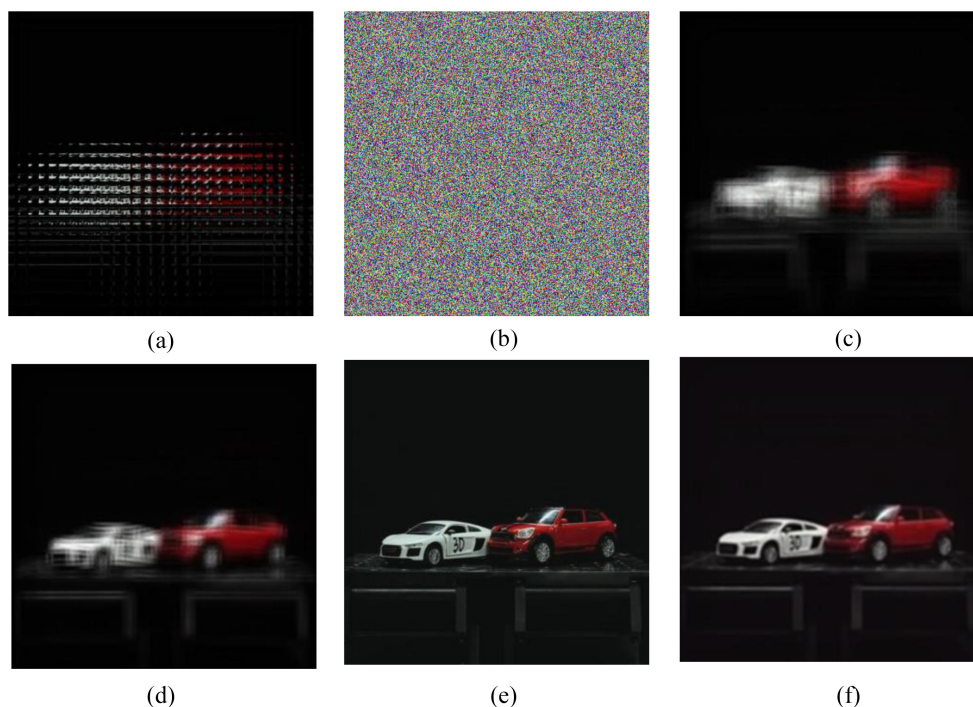


Fig. 5. (a) Original elemental image, (b) the cipher image generated by the proposal, (c) the recovered scene using proposal (80mm), (d) the recovered plane image using proposal (90 mm), (e) the recovered plane image using proposal (100 mm), (f) the recovered plane image with the CIIR method (100 mm).

the average encryption time of using the proposed algorithm to encrypt image (with the size of 355×355) is 0.886s.

To confirm the visual quality of the recovered scene, we utilize the peak signal-to-noise ratio (PSNR) to objectively measure the quality of the decrypted scene. The PSNR can be calculated by the following formula:

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

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

where M and N represent the size of image, E and E' are the original and recovered scenes, respectively.

The PSNR value of the recovered scene generated by the proposed method is 38.56 dB, and that of the recovered scene obtained by the traditional CIIR method is 34.68 dB, respectively. It confirms that the proposed method can obtain a decrypted scene with high visual quality.

4.1. Key Security Analysis

According to cryptanalysis theory, a qualified encryption system must require a large key space to resist brute force attacks. In addition to the depth of reconstruction, CA algorithm further increases the key space of the cryptosystem. For a 1D CA with n -cells, two states, and m -site neighborhood, its key space is approximately $2^{2M} \times 2^N \times 2^{2N}$ ($M = 355$, $N = 355$). Hence, the total key space possessed by the scheme is far greater than the security requirement of $2^{100} (\approx 10^{30})$, it means that the method can effectively resist brute force attacks.

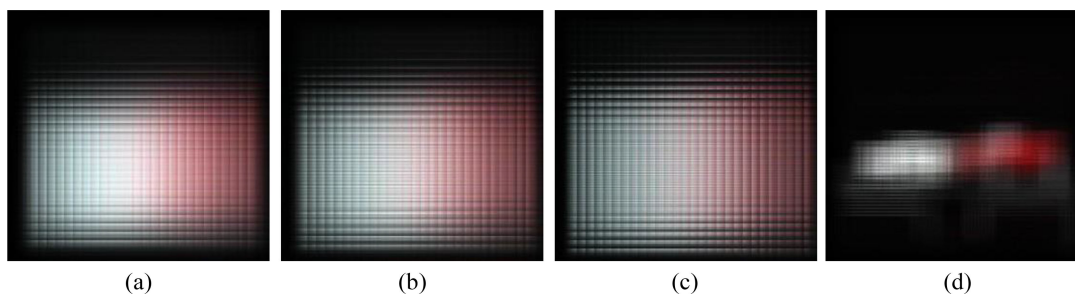


Fig. 6. Reconstructed plane image with the partial wrong keys: (a) wrong CA sequence M1, (b) wrong CA sequence M2, (c) wrong CA sequence M3, (d) incorrect reconstruction depth (50 mm).

TABLE 3
PSNR, MSE and Information Entropy of the Ciphered Image With Different Methods

Different methods	PSNR(dB)	MSE	Information entropy
DNA-based method	12.17	3946	7.8575
CA-based method	11.02	5136	7.8767
Proposed method	10.51	5784	7.9995

At the same time, the cryptosystem must be highly sensitive to key change. When the key changes slightly, the corresponding decrypted image becomes completely different. As shown in the following example, the sensitivity of the proposed scheme to key conversion can be seen. Fig. 5 shows the restored plane scene with partial wrong key. Figs 6(a)-6(c) show plane scenes reconstructed with different random sequences generated by wrong CA rules. Fig. 6(d) illustrates the recovered plane images with the wrong distance. From the result, it can be seen that the decrypted scene is very different from the ordinary scene, and the original information is not visually identifiable. The results prove that proposed scheme is sensitive to the key change.

Information entropy is an important characteristic for evaluating the randomness of an encryption system [40]. The information entropy of the ciphertext can be calculated by the following formula [31]:

$$H_i(E) = \sum_{i=0}^{2^N-1} P(E) \log_2(P(E)), \quad (12)$$

where $P(E)$ is the probability of E . From the theory of information entropy, we can know that the closer the value of information entropy is to 8, the better the randomness of the image. And the entropy of the encrypted image is 7.9995, which proves that the cryptographic system can effectively resist entropy attacks.

In order to further verify the security of the proposed algorithm, we compare our method with the DNA-based encryption algorithm and CA-based encryption algorithm. In DNA-based algorithm, DNA encoding and DNA decoding operations are performed using fixed rules (key1 = 2, key2 = 8), and a one-dimensional chaotic sequence with parameters ($x_0 = 0.9058$, $u_0 = 3.6246$) is used to complete DNA complementary operation and bit pixel scrambling operations. In CA-based algorithm, a one-dimensional CA mask with rules (150; 90; 150; 90; 90; 90; 150; 90) is used to obtain encrypted image. Table 3 is the comparison of the PSNR, MSE and Information entropy results of the ciphertext image using our proposed algorithm and some other methods. It can be seen from the results that the PSNR of the ciphertext generated by our proposed method is smaller,

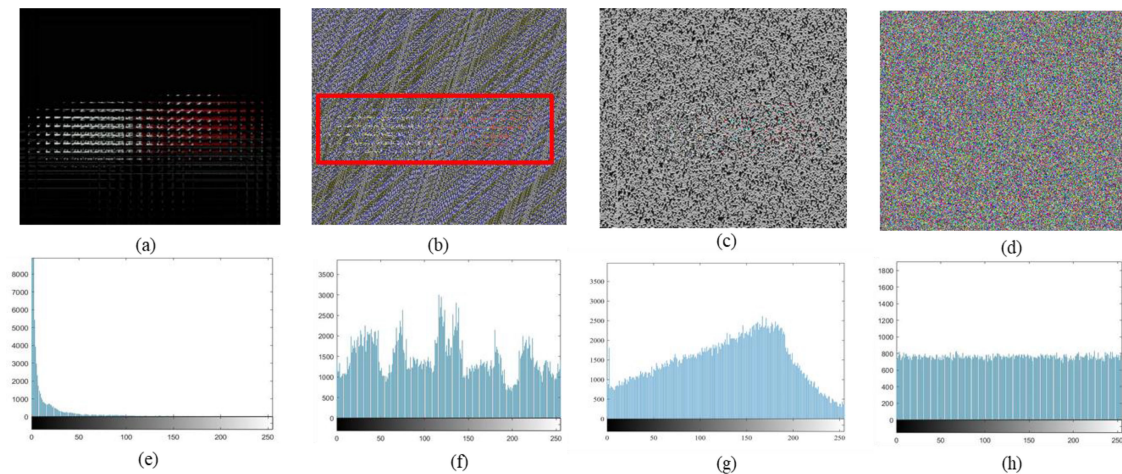


Fig. 7. (a) Original elemental image, (b) the cipher image produced by the DNA-based scheme, (c) the cipher image produced by the CA-based scheme, (d) the cipher image produced by the proposed scheme, (e) the histogram of (a), (f) the histogram of (b), (g) the histogram of (c), (h) the histogram of (d).

and the information entropy is closer to 8, so the randomness of the ciphertext is better. It proves that our proposed method has good security.

4.2. Statistical Analysis

In order to confirm the statistical characteristics of our CA-based DNA encryption scheme, we compare our method with the DNA-based encryption algorithm and CA-based encryption algorithm. Fig. 7(b) illustrates the cipher image produced by a DNA encoding algorithm. From the red frame in this figure, we can see the patterns of the object, which can provide hints for attacking encryption method. To address this problem, we introduce a CA algorithm to evenly distribute the energy of obvious patterns. As shown in Fig. 7(d), the cipher image generated by the proposed encryption approach, which is a uniformly distributed noise-like image. Compared with the image generated by the CA algorithm, as shown in Fig. 7(c), the ciphertext generated by our proposed method is more uniform. It effectively solves the silhouette problem.

To prevent data from being illegally obtained by attackers, it is of great significance to ensure that the cipher-text and the plain-text are not statistically similar. As an important tool, image histogram is applied to analyze the statistical properties of encryption method. Fig. 7(e) illustrates the histogram of the element image. Fig. 7(f) illustrates the histogram of the cipher image produced by the DNA-based encryption algorithm. Fig. 7(g) illustrates the histogram of the cipher image produced by the CA-based encryption algorithm. And Fig. 7(h) shows the histogram of the cipher image generated by proposed approach. The results verify that the histogram of cipher image produced by proposed method becomes flatter. Therefore, the proposed algorithm brings effective performance against statistical attacks.

Meanwhile, the auto-correlation between the pixels of the cipher image should be weak. Fig. 8(a) shows that there is strong auto-correlation between adjacent pixels in the original scene, and Fig. 8(b) illustrates the auto-correlation of the cipher image generated by the DNA-based algorithm. Fig. 8(c) illustrates the auto-correlation of the cipher image generated by the CA-based algorithm and Fig. 8(d) shows the auto-correlation of the encrypted image generated using the proposed method, which certifies that the auto-correlation of this image is weaker than that of other images. The results undoubtedly verify that the proposed encryption method has qualified decorrelation performance to resist attacks.

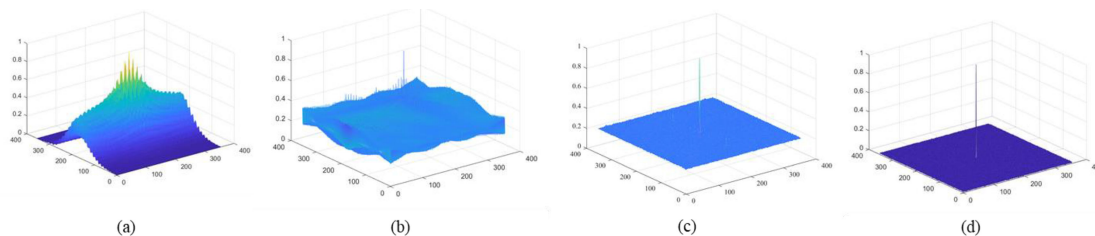


Fig. 8. Autocorrelation of the image (R-content): (a) original scene, (b) the cipher image of the DNA-based method, (c) the cipher image of the CA-based method, (d) the cipher image of the proposed method.

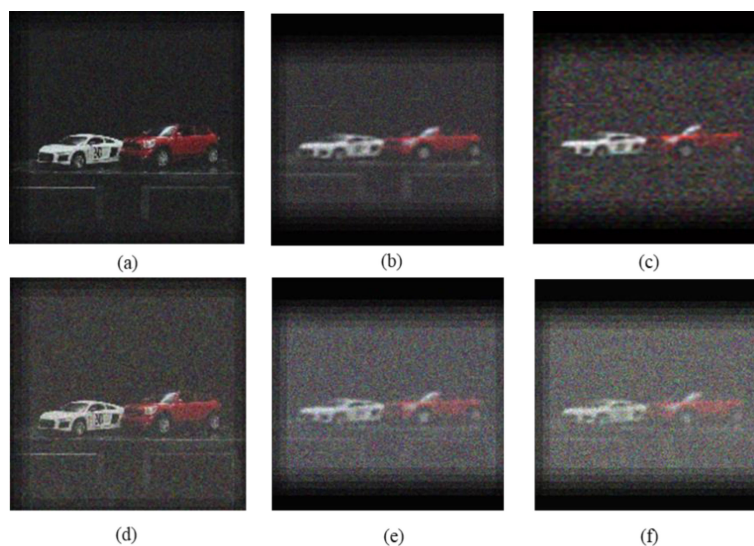


Fig. 9. Reconstructed scenes against different density Gaussian noise attacks: (a) the proposed scheme (density $\sigma = 0.1$), (d) the proposed scheme (density $\sigma = 0.2$), (b) the DNA-based scheme (density $\sigma = 0.1$), (e) the DNA-based scheme (density $\sigma = 0.2$), (c) the CA-based scheme (density $\sigma = 0.1$), (f) the CA-based scheme (density $\sigma = 0.2$).

TABLE 4
PSNRs of Decrypted Scenes Against Attacks With Different Schemes

Attacks	Proposed method			DNA-based method			CA-based method		
	R(dB)	G(dB)	B(dB)	R(dB)	G(dB)	B(dB)	R(dB)	G(dB)	B(dB)
Gaussian ($\sigma=0.1$)	25.13	25.20	24.68	15.51	15.34	15.26	13.67	13.56	13.45
Gaussian ($\sigma=0.2$)	16.26	15.06	16.87	12.76	12.15	12.06	11.55	11.34	11.51
Salt &pepper ($\sigma=0.1$)	29.62	29.43	29.78	23.76	23.87	23.54	21.66	21.43	21.21
Salt &pepper ($\sigma=0.2$)	21.62	22.07	22.26	15.23	15.19	15.36	13.54	13.32	13.22
Speckle ($\sigma=0.1$)	27.01	27.63	27.34	22.98	22.06	22.84	20.28	20.16	20.34
Speckle ($\sigma=0.2$)	23.77	22.56	22.72	17.15	17.09	17.48	15.18	15.69	15.48

4.3. Robustness Analysis

A qualified encryption approach also should withstand a given mass attacks. We analyze the robustness to some attacks for encrypted image by comparing our proposed CA-based DNA encryption scheme with the conventional DNA-based scheme. Fig. 7 illustrates the results of decrypted scenes with different density Gaussian noise attacks. Figs 9(a) and 9(d) denote the recovered scenes by proposed approach. Figs 9(b) and 9(e) show the recovered scenes with DNA-based scheme. And Figs. 9(c) and 9(f) show the recovered scenes with CA-based scheme. From the results shown in Fig. 9, although, the encrypted images are severely affected by the noise attack, the proposed method can clearly identify the original scene information.

Next, we utilize PSNRs to quantitatively measure the quality of the recovered scene against noise attacks. Table 4 records the PSNRs calculated using different encryption schemes. These results indicate that the proposed scheme brings better robustness to attacks.

5. Conclusion

In conclusion, we presented an optical encryption approach using integral imaging and CA-DNA algorithm, which resolve the silhouette problem of cipher image in the traditional DNA encoding algorithms. The DNA random complementary operation and pixel scrambling can further improve the security of the encryption scheme. Meanwhile, the modified reconstruction method is applied to enhance the visual quality of the recovered scenes. We also analyze the robustness of the proposed scheme against different attacks. Experimental results verify that the encryption scheme has better capability than the DNA-based algorithm.

References

- [1] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, 2014.
- [2] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Opt. Laser Eng.*, vol. 107, pp. 370–379, 2018.
- [3] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, 2013.
- [4] X. Y. Li *et al.*, "Multiple-image encryption based on compressive ghost imaging and coordinate sampling," *IEEE Photon. J.*, vol. 8, no. 4, Aug. 2016, Art. no. 3900511.
- [5] X. Li, D. Xiao, and Q. H. Wang, "Error-free holographic frames encryption with CA pixel-permutation encoding algorithm," *Opt. Laser Eng.*, vol. 100, pp. 200–207, 2018.
- [6] Y. Qin, Z. Wang, H. Wang, Q. Gong, and N. Zhou, "Robust information encryption directive-imaging-based scheme with special phase retrieval algorithm for a customized data container," *Opt. Laser Eng.*, vol. 105, pp. 118–124, 2018.
- [7] W. Chen, X. Chen, and C. J. R. Sheppard, "Optical color-image encryption and synthesis using coherent diffractive imaging in the fresnel domain," *Opt. Exp.*, vol. 20, no. 4, pp. 3853–3865, 2012.
- [8] Y. Wang, C. Quan, and C. J. Tay, "Cryptanalysis of an information encryption in phase space," *Opt. Laser Eng.*, vol. 85, pp. 65–71, 2016.
- [9] L. Chen, G. Chang, B. He, H. Mao, and D. Zhao, "Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition," *Opt. Laser Eng.*, vol. 88, pp. 221–232, 2017.
- [10] W. Chen, "Optical multiple-image encryption using three-dimensional space," *IEEE Photon. J.*, vol. 8, no. 2, Apr. 2016, Art. no. 6900608.
- [11] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, 2016.
- [12] S. Hong, J. Jang, and B. Javidi, "Three-dimensional volumetric object reconstruction using computational integral imaging," *Opt. Exp.*, vol. 12, no. 3, pp. 483–491, 2004.
- [13] D. Shin, and H. Yoo, "Image quality enhancement in 3D computational integral imaging by use of interpolation methods," *Opt. Exp.*, vol. 15, no. 19, pp. 12039–12049, 2007.
- [14] Y. Wang, X. Wang, J. Zhang, S. Yu, Q. Zhang, and B. Guo, "Resolution improvement of integral imaging based on time multiplexing sub-pixel coding method on common display panel," *Opt. Exp.*, vol. 22, no. 15, pp. 17897–17907, 2014.
- [15] Y. Wang, Y. Shen, Y. Lin, and B. Javidi, "Extended depth-of-field 3D endoscopy with synthetic aperture integral imaging using an electrically tunable focal-length liquid-crystal lens.," *Opt. Lett.*, vol. 40, no. 15, pp. 3564–3567, 2015.
- [16] A. Stern, and B. Javidi, "Three-dimensional image sensing and reconstruction with time-division multiplexed computational integral imaging," *Appl. Opt.*, vol. 42, no. 35, pp. 7036–7042, 2003.
- [17] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, pp. 1021–1024, 1994.

- [18] X. Xiao, B. Javidi, M. Martinez-Corral, and A. Stern, "Advances in three-dimensional integral imaging: Sensing, display, and applications," *Appl. Opt.*, vol. 52, no. 4, pp. 546–560, 2013.
- [19] Z. Xiong, Q. H. Wang, Y. Xing, H. Deng, and D. Li, "An active integral imaging system based on multiple structured light method," *Opt. Exp.*, vol. 23, no. 21, pp. 27095–27104, 2015.
- [20] J. Wang, X. Xiao, and B. Javidi, "Three-dimensional integral imaging with flexible sensing," *Opt. Lett.*, vol. 39, no. 24, pp. 6855–6858, 2014.
- [21] X. Li, and I. Lee, "Robust copyright protection using multiple ownership watermarks," *Opt. Exp.*, vol. 23, no. 3, pp. 3035–3046, 2015.
- [22] I. Muniraj, B. Kim, and B. Lee, "Encryption and volumetric 3D object reconstruction using multi-spectral computational integral imaging," *Appl. Opt.*, vol. 53, no. 27, pp. G25–G32, 2014.
- [23] S. Hong, J. Jang, and B. Javidi, "Three-dimensional volumetric object reconstruction using computational integral imaging," *Opt. Exp.*, vol. 12, no. 3, pp. 483–491, 2004.
- [24] X. Li *et al.*, "Designing optical 3D images encryption and reconstruction using monospectral synthetic aperture integral imaging," *Opt. Exp.*, vol. 26, no. 9, pp. 11084–11099, 2018.
- [25] X. Li *et al.*, "Optical encryption via monospectral integral imaging," *Opt. Exp.*, vol. 25, no. 25, pp. 31516–31527, 2017.
- [26] A. Markman, J. Wang, and B. Javidi, "Three-dimensional integral imaging displays using a quick-response encoded elemental image array," *Optica*, vol. 5, no. 1, pp. 332–335, 2014.
- [27] J. D. Watson, and F. H. C. Crick, "A structure for deoxyribose nucleic acid," *Nature*, vol. 171, no. 4356, pp. 737–738, 1953.
- [28] S. L. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201714.
- [29] H. Liu, X. Wang, and A. Kadir, "Image encryption using dna complementary rule and chaotic maps," *Appl. Soft Comput. J.*, vol. 12, pp. 1457–1466, 2012.
- [30] M. K. A. Guesmi, R. Farah, and M. Samet, "A novel chaos-based image encryption using dna sequence operation and secure hash algorithm sha-2," *Nonlinear Dynam.*, vol. 83, pp. 1123–1136, 2016.
- [31] X. Fu, B. Liu, Y. Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using dna encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, Jun. 2018, Art. no. 3900515.
- [32] Y. Q. Zhang, X. Y. Wang, J. Liu, and Z. L. Chi, "An image encryption scheme based on the mlncml system using dna sequences," *Opt. Lasers Eng.*, vol. 82, pp. 95–103, 2016.
- [33] X. Y. Wang, H. L. Zhang, and X. M. Bao, "Color image encryption scheme using cml and dna sequence operations," *Bio Syst.*, vol. 144, pp. 18–26, 2016.
- [34] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, 2019.
- [35] T. Wang, and M. H. Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Opt. Lasers Tech.*, vol. 132, 2020, Art. no. 106355.
- [36] B. Aashiq, R. Amirtharajan, and D. Ravichandran, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Med. Biol. Eng. Comput.*, vol. 59, pp. 589–605, 2021.
- [37] X. Wang, and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence," *Opt. Lasers Eng.*, vol. 137, no. 11, 2021, Art. no. 106393.
- [38] S. J. Cho, U. S. Choi, and Y. H. Hwang, "Cell automata," *Lect. Notes Comput. Sci.*, vol. 3305, pp. 31, 2004.
- [39] M. H. Niyat, A. Y. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Opt. Lasers Eng.*, vol. 90, pp. 225–237, 2017.
- [40] C. Li, B. Feng, and J. Li, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.
- [41] X. Li, S. Kim, and I. Lee, "3D image encoding in FT domain based on CGII algorithm," *Appl. Math. Model.*, vol. 39, no. 14, pp. 3899–3912, 2015.
- [42] M. Tsompanas, G. Sirakoulis, and A. Adamatzky, "Evolving transport networks with cellular automata models inspired by slime mould," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 1887–1899, Sep. 2015.
- [43] X. Li, C. Q. Li, and I. Lee, "Chaotic image encryption using pseudo-random masks and pixel mapping," *Signal Process.*, vol. 125, pp. 48–63, 2016.
- [44] M. Bidlo, "On routine evolution of complex cellular automata," *IEEE Trans. Evolut. Comput.*, vol. 20, no. 5, pp. 742–754, Oct. 2016.
- [45] X. Li, S. Kim, and Q. H. Wang, "Designing three-dimensional cellular automata-based video authentication with an optical integral imaging generated memory-distributed watermark," *IEEE J. Sel. Topics Sign. Process.*, vol. 11, no. 7, pp. 1200–1212, Oct. 2017.
- [46] M. Li, D. Lu, W. Wen, H. Ren, and Z. Yushu, "Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata," *IEEE Access*, vol. 6, pp. 47102–47111, 2018.