frontiers in Physics

ORIGINAL RESEARCH
published: 07 March 2022
doi: 10.3389/fphy.2022.844966

A Novel 3D Image Encryption Based on the Chaotic System and RNA Crossover and Mutation

Ran Chu[1,2], *Shufang Zhang*[1]* *and Xianpeng Gao*[3]

[1]Information Science and Technology College, Dalian Maritime University, Dalian, China, [2]Information Science and Engineering College, Dalian Polytechnic University, Dalian, China, [3]Tokai Carbon Dalian Co., Ltd., Dalian, China

In this paper, a novel 3D image encryption based on the memristive chaotic system and RNA crossover and mutation is proposed. Firstly, the dynamic characteristics of the nonlinear system with two memristors are analyzed, including phase diagrams, Lyapunov exponential spectrums, and bifurcation diagrams. According to the merged image of three 3D images, the initial values of the memristive chaotic system are generated by SHA-256. Then the vertex coordinates are scrambled and diffused by 3D Arnold matrix and chaotic sequences. Finally, according to the dynamical encoding and decoding rules, crossover and RNA mutation are designed to confuse and diffuse the vertex coordinates. Throughout the encryption process, the Arnold matrix, RNA encoding and decoding rules, and crossover and mutation algorithms are determined by the memristive chaotic system. The experimental results verify that the proposed cryptosystem could encrypt three 3D images at the same time and resist various attacks effectively, and has good security performance.

Keywords: 3D images, memristive chaotic system, crossover, RNA mutation, 3D Arnold matrix

OPEN ACCESS

Edited by:
Jun Mou,
Dalian Polytechnic University, China

Reviewed by:
Fei Yu,
Changsha University of Science and Technology, China
Hongjun Liu,
University of Jinan, China

***Correspondence:**
Shufang Zhang
sfzhang@dlmu.edu.cn

Specialty section:
This article was submitted to Interdisciplinary Physics, a section of the journal Frontiers in Physics

Received: *29 December 2021*
Accepted: *18 January 2022*
Published: *07 March 2022*

Citation:
Chu R, Zhang S and Gao X (2022) A Novel 3D Image Encryption Based on the Chaotic System and RNA Crossover and Mutation. Front. Phys. 10:844966. doi: 10.3389/fphy.2022.844966

INTRODUCTION

With the development of wireless network and multimedia technology, more images are transmitted on the network. Among them, 3D printing has been widely used in medical, military, marine, and many other fields due to its available price. It can be predicted that the 3D images will be as popular as color images and videos in the future [1–3]. However, the 3D images can be downloaded easily, and 3D objects can be printed out without permission from the original providers. In order to prevent the attacks by unauthorized users, the 3D images should be encrypted before being stored and transmitted. Unlike the traditional files, the 3D image files have enormous data and special storage format, so the traditional encryption algorithms such as DES and AES cannot protect them efficiently [4–8]. Therefore, it is necessary to research high-level encryption technology for 3D images, and there are few researches on this field at present.

In the era of big data, some traditional image cryptosystems can be easily cracked by cloud computing. Therefore, it is necessary to propose a more secure image cryptosystem to meet the current requirements and protect the privacy of users. Chaotic systems have many significant features, including ergodicity, randomness, and sensitivity to initial values, which make them suitable for image encryption [9–22]. It is important to point out that the nonlinearity of memristor element enables the memristor circuits to generate chaotic signal and various chaotic attractors and exhibit abundant nonlinear phenomena [11, 23, 24]. Peng et al. [25] presented a dimensional chaotic map based on the discrete memristor, which can enlarge the hyperchaotic region and enhance complexity.

TABLE 1 | The format of the STL file

Vertex				Face	
Number	***x*-axis**	***y*-axis**	***z*-axis**	**Number**	**Elements in face**
1	$V_{1,x}$	$V_{1,y}$	$V_{1,z}$	1	$(V_{1,x}, V_{1,y}, V_{1,z})$
2	$V_{2,x}$	$V_{2,y}$	$V_{2,z}$	2	$(V_{2,x}, V_{2,y}, V_{2,z})$
3	$V_{3,x}$	$V_{3,y}$	$V_{3,z}$	3	$(V_{3,x}, V_{3,y}, V_{3,z})$
...	...	...	...	...	...
n	$V_{n,x}$	$V_{n,y}$	$V_{n,z}$	*n*	$(V_{n,x}, V_{n,y}, V_{n,z})$

Chen et al. [26] proposed a pseudorandom number generator by three kinds of four-wing memristive hyperchaotic systems, the dynamical characteristics are sensitive and complex. Ma et al. [27] proposed a chaotic circuit based on two memristors, which has rich dynamical behaviors and is suitable for image encryption and secure communication.

With the development of the chaos theory, the fusion of chaotic system and cryptography has become an important solution to ensure image security [28–32]. Based on the chaotic systems, many image encryption schemes are designed by optical transformation [33, 34], compressive sensing [35], DNA and RNA computing [36–41], cellular automata [42], etc. Among them, RNA computing can increase information density, improve parallelism, and reduce energy consumption, so it has become a research hotspot recently [43–45]. Abbasi et al. [46] proposed a cryptosystem based on amino acid, RNA codons, and evolutionary chaotic model, and the performance of the cryptosystem is improved by biomolecules and the imperialist competition algorithm. Jarjar et al. [47] presented a method that uses several genetic and biological features of DNA and RNA to encrypt color images and model mathematical problems as biological ones. Zhang et al. [48] proposed an image cryptosystem based on hyperchaotic system and RNA operation, which could resist various attacks. However, all the researches above are based on the RNA encoding/decoding law; the calculation results between the RNA bases are easy to predict, increasing the risk of cracking. Therefore, the traditional RNA scheme could be improved.

Based on the above analyses, a novel 3D image cryptosystem is proposed in this paper. The rest of the parts are organized as follows. In *Preprocessing of the 3D Model*, the preprocessing of 3D model data is described. In *Chaotic System*, the memristive chaotic system is introduced and its dynamical characteristics are illustrated. In *Encryption Scheme*, the SHA-256 algorithm, improved 3D Arnold algorithm, and RNA level encryption algorithm are described. In *Performance Analysis*, the security performance and experimental results are evaluated through the key analysis, statistical analysis, information entropy, and robust security analysis. In *Section Conclusion*, some important conclusions are obtained.

PREPROCESSING OF THE 3D MODEL

Stereolithography (STL) is the standard technology file of current 3D printing technology, which is used to describe the triangulated surface geometry of a 3D model by vertices, faces, and unit normal. The format of the STL file is shown in **Table 1**. The *x*, *y*, and *z* coordinates of the vertices determine the shape of the 3D model, just like the RGB pixels of a color image file. Therefore, 3D images could be transformed into 2D objects, and the coordinates of the vertices are a protected object.

Each vertex consists of *x*, *y*, and *z* coordinates (floating point value of at least 96 bit). To enable fast processing with accurate results, all data should be normalized first. Considered the efficiency requirement, the Min–Max Normalization is used to normalize the coordinate data, and the scale criterion is used to rescale the coordinate data, as follows:

$$V' = R_{\min} + \frac{V - V_{\min}}{V_{\max} - V_{\min}} \times (R_{\max} - R_{\min}) \tag{1}$$

where V' is the normalized coordinate, V is the original coordinate, $V_{\min}$ and $V_{\max}$ are minimum and maximum original coordinates, and $R_{\min}$ and $R_{\max}$ are the selected range, ranging from −255 to 255.

After extracting the symbol matrix from the floating point number matrix, the positive array is obtained. Then, it is decomposed into integer matrix V_i and fractional matrix V_f.

CHAOTIC SYSTEM

Recently, a chaotic circuit based on two memristors was proposed, which has multiple attractor coexistence and state transition, defined as

$$\begin{cases} \dot{x} = \frac{1}{L} \cdot y - \frac{1}{La_1} \cdot \frac{x}{z} \\ \dot{y} = -\frac{1}{C} \cdot x - \frac{a_2}{C} \cdot wy \\ \dot{z} = \left(\frac{x}{a_1 z}\right)^2 - b_1 \\ \dot{w} = y^2 - b_2 \end{cases} \tag{2}$$

where *x*, *y*, *z*, and *w* represent the system states variables; *L*, *C*, a_1, a_2, b_1, and b_2 are system parameters. With the variation of parameters, the system has seven types of attractors. Set $L = 0.025$, $C = 0.025$, $a_1 = 5.8$, $a_2 = 0.825$, $b_1 = 1.85$, $b_2 = 10$, and the initial values are (1, 3, 1, −0.7). **Figure 1** shows the phase diagrams. The Lyapunov exponential spectrums and bifurcation diagrams are presented in **Figure 2**.

When $a_1 \in (4.5,6.5)$, $a_2 \in (0.7,0.9)$, $b_1 \in (1.7,2.2)$, and $b_2 \in (9,11)$, the bifurcation diagram shows that the system changes from periodic to chaotic, the chaotic states are widely distributed, and the system has complex dynamic characteristics, which can also be verified by the Lyapunov exponential spectrum. At least one Lyapunov exponent in a chaotic system is greater than zero, and the largest Lyapunov exponent in a Lyapunov diagram is always positive, that is, the system is in the chaotic state. These characteristics of the chaotic system make it suitable for image encryption.

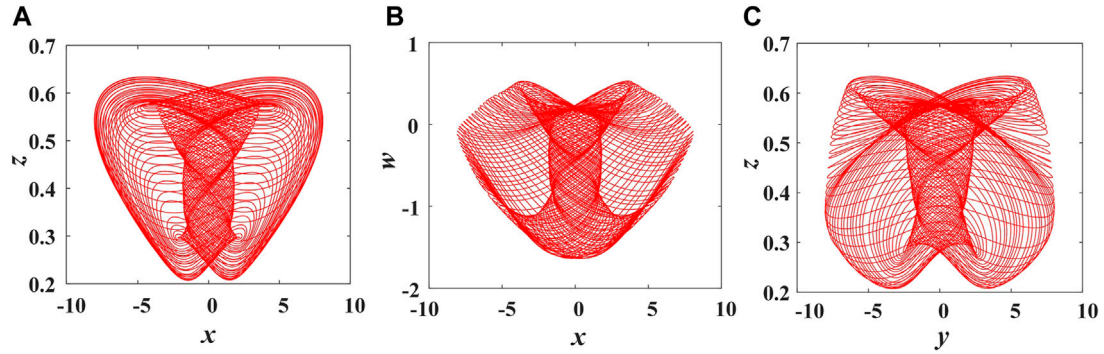

FIGURE 1 | The phase diagrams. **(A)** *x-z* plane, **(B)** *x-w* plane, **(C)** *y-z* plane.

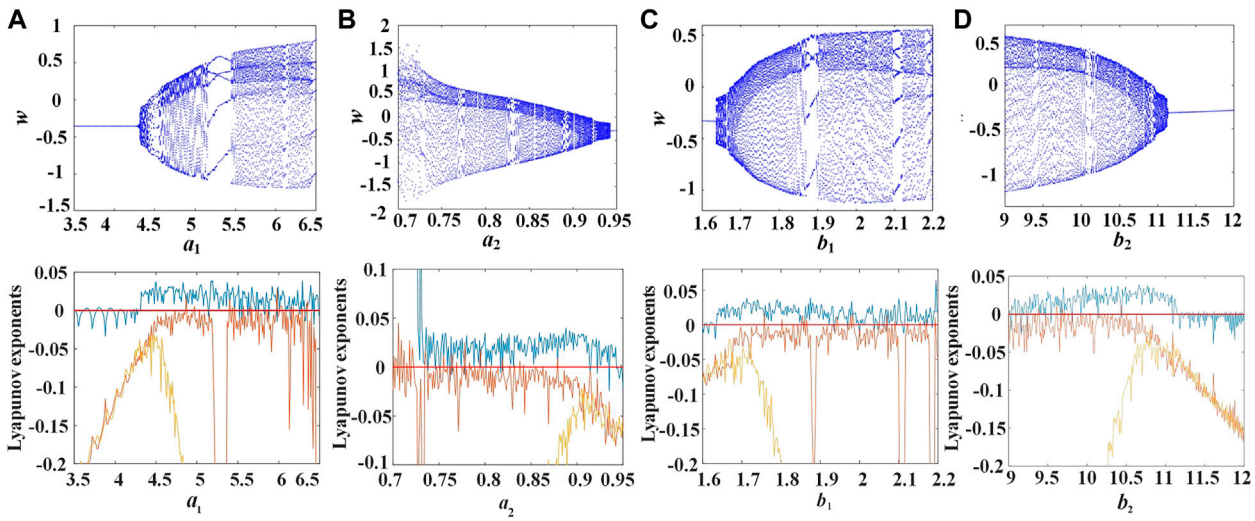

FIGURE 2 | Lyapunov exponent spectrums and bifurcation diagrams. **(A)** $a_1 \epsilon (3.5,6.5)$, **(B)** $a_2 \epsilon (0.7,0.95)$, **(C)** $b_1 \epsilon (1.6,2.2)$, **(D)** $b_2 \epsilon (9,12)$.

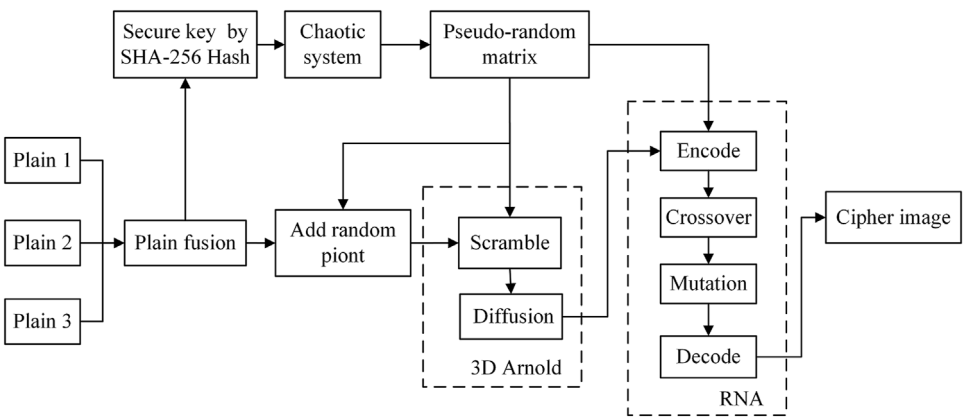

FIGURE 3 | The flowchart of encryption algorithm.

ENCRYPTION SCHEME

The encryption process is described, including the SHA-256 algorithm, improved 3D Arnold algorithm, and RNA operations. The flowchart is shown in **Figure 3**.

SHA-256 Algorithm

To improve the security, the SHA-256 is used in the encryption algorithm. Three 3D images are merged together by the method of 3D stereo arrangement. Therefore, different images and different orders will generate different hash values and then obtain different initial conditions, thus producing different chaotic sequences.

Step 1: Based on the merged image I, the 256-bit hash value is generated by the SHA-256 algorithm and divided into eight-bit blocks (total 64 group bit blocks). Thus, the stream key is obtained by XOR operation:

$$H(i) = h(2i) \oplus h(2i-1) \tag{3}$$

where $i \in (1, 32)$. The slight disturbance is generated as follows

$$\begin{cases} k_1 = 10^{-15} \times \mathrm{sum}(H(1{:}\ 8) \oplus H(9{:}\ 16)) \\ k_2 = 10^{-15} \times \mathrm{sum}(H(17{:}\ 24) \oplus H(25{:}\ 32)) \\ k_3 = 10^{-15} \times \mathrm{sum}(H(1{:}\ 8) \oplus H(25{:}\ 32)) \\ k_4 = 10^{-15} \times \mathrm{sum}(H(9{:}\ 16) \oplus H(17{:}\ 24)) \\ k_5 = 10^{-15} \times \mathrm{sum}(V) \end{cases} \tag{4}$$

Step 2: Input the initial condition as the key. Then, the adjusted initial conditions are generated.

$$\begin{cases} x = x_0 + (k_1 + k_2) \\ y = y_0 + (k_2 + k_3) \\ z = z_0 + (k_3 + k_4) \\ w = w_0 + (k_4 + k_5) \end{cases} \tag{5}$$

where x, y, z, and w are adjusted initial values; x_0, y_0, z_0, and w_0 are given values without disturbance. Suppose the plaintext size is $M \times N$, according to the adjusted initial conditions, the chaotic system is iterated $(n + M \times N)$ times. To increase the sensitivity of initial values, discard the front n times values. The sequences X, Y, Z and W are generated.

$$\begin{cases} X = \mathrm{mod}(\mathrm{floor}(\mathrm{abs}(x \times 10^{15})), 256) \\ Y = \mathrm{mod}(\mathrm{floor}(\mathrm{abs}(y \times 10^{15})), 256) \\ Z = \mathrm{mod}(\mathrm{floor}(\mathrm{abs}(z \times 10^{15})), 256) \\ W = \mathrm{mod}(\mathrm{floor}(\mathrm{abs}(w \times 10^{15})), 256) \end{cases} \tag{6}$$

Thus, the chaotic sequences are affected by hash value of plaintext, which can improve the random adaptive ability.

Improved 3D Arnold Algorithm

On the basis of chaotic sequence, irrelevant vertices are added to ensure security, and then, an improved 3D Arnold cat map is performed for scrambling and diffusion. In the encryption scheme, the integer matrix is confused and diffused. In order to save the encryption time, the fractional matrix is only treated by diffusion.

Step 1: In the 3D Arnold matrix, the calculation principle of control parameters depends on the chaotic sequence, as shown in the formula:

$$\begin{cases} S_A = \lfloor a \cdot x + c \cdot y - y \cdot z \rfloor \\ S_B = \lfloor z \cdot (x-1) - b \cdot y \rfloor \\ S_C = \lfloor a \cdot y + c \cdot z - x \cdot z \rfloor \\ S_D = \lfloor x \cdot (y-1) - b \cdot z \rfloor \\ S_E = \lfloor a \cdot z + c \cdot x - x \cdot y \rfloor \\ S_F = \lfloor y \cdot (z-1) - b \cdot x \rfloor \end{cases} \tag{7}$$

where a, b, and c are specified parameters.

Step 2: The 3D Arnold matrix is obtained by multiplication of cubic matrices, as follows:

$$A = \begin{bmatrix} 1 & 0 & S_A \\ 0 & 1 & 0 \\ S_B & 0 & S_A \times S_B + 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & S_C \\ 0 & S_D & S_C \times S_D + 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & S_E & 0 \\ S_F & S_E \times S_F + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{8}$$

Step 3: The integer matrix and fractional matrix are scrambled by the 3D Arnold matrix. The scrambled coordinate positions are generated as follows:

$$\begin{bmatrix} i_A \\ j_A \\ k_A \end{bmatrix} = A \cdot \begin{bmatrix} i \\ j \\ k \end{bmatrix} \mathrm{mod} \begin{bmatrix} N_{\mathrm{row}} \\ N_{\mathrm{column}} \\ N_{\mathrm{graph}} \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \tag{9}$$

where (i, j, k) is the original position; N_{row}, N_{column}, and N_{gragh} are the number of rows, columns, and graphs. (i_A, j_A, k_A) is the scrambled position. After each vertex coordinate is shifted with the replacement vertex, the scrambled image is obtained.

Step 4: The integer matrix is diffused by the 3D Arnold matrix, as follows:

$$\begin{bmatrix} AV_i(i,j,k) \\ AV_i(i_A, j_A, k_A) \\ AV_i(i', j', k') \end{bmatrix} = A \cdot \begin{bmatrix} V_i(i,j,k) \\ V_i(i_A, j_A, k_A) \\ V_i(i', j', k') \end{bmatrix} \mathrm{mod} \begin{bmatrix} 256 \\ 256 \\ 256 \end{bmatrix} \tag{10}$$

where $V_i(i, j, k)$ and $V_i(i_A, j_A, k_A)$ are scrambled values of the previous step, and $V_i(i', j', k')$ is the diffused value of the previous round. $AV_i(i, j, k)$, $AV_i(i_A, j_A, k_A)$, and $AV_i(i', j', k')$ are the values after diffusion. After each coordinate in the matrix is transformed, the diffused image matrix I_1 is obtained.

With the improved 3D Arnold algorithm, the matrix can be scrambled and diffused simultaneously, which could save the encryption time and reduce the computational complexity.

RNA Encryption Algorithm

The RNA encryption algorithm aims to confuse and diffuse the vertex coordinates completely. The bio-inspired chaotic encryption algorithm can be divided into encoding, diffusion, crossover, mutation, and decoding stages.

Step 1: RNA coding rules. The RNA sequence is constructed by four nitrogen bases, namely, Adenine (A), Guanine (G), Uracil (U), and Cytosine (C). The complementary coding rules are shown in **Table 2**. Besides, **Table 3** shows the RNA operation rules.

Step 2: RNA diffusion. The rules of coding and operation are both determined by chaotic sequences. Convert the matrix I_1 and chaotic sequence to a binary matrix of size $M \times N \times 8$. Then,

TABLE 2 | The RNA encoding rules

Rule	1	2	3	4	5	6	7	8
00	A	A	U	U	G	G	C	C
01	C	G	C	G	U	A	U	A
10	G	C	G	C	A	U	A	U
11	U	U	A	A	C	C	G	G

TABLE 3 | The RNA operation rules

+	A	C	G	U	–	A	C	G	U
A	A	C	G	U	A	A	U	G	C
C	C	G	U	A	C	C	A	U	G
G	G	U	A	C	G	G	C	A	U
U	U	A	C	G	U	U	G	C	A

according to the dynamic coding rules, the plaintext is transformed into an RNA sequence of size $M \times N \times 4$. The disorder sequence is obtained by substituting base pairs under the complementary rule. Then, the diffused cipher sequence P is obtained.

Step 3: Gene crossover. Crossover, also known as gene recombination or hybridization, is the exchange of genetic material at the same location of two chromosomes to generate two new recombinant chromosomes. In 3D image encryption algorithm, the vertex coordinates are exchanged to accomplish the crossover, similar to the chromosome swapping in biology. The sequence P is divided into two sequences P_1 and P_2 of equal length. Transform the chaotic sequence ($x \oplus w$) into a binary sequence that determines the crossover position of the unit: 1 means exchange, 0 means non-exchange, as shown in **Figure 4**. When the crossover is complete, merge the two sequences.

Step 4: RNA mutation. Codon refers to a triplet sequence of nucleotide residues in RNA that encodes a specific amino acid during protein synthesis. Mutations are certain replication errors that occur during replication, leading to the formation of new chromosomes. In 3D image cryptosystem, the changes in vertex coordinates correspond to mutation in biology. According to the chaotic sequence, two mutation units are found and defined in RNA sequence, as shown in **Figure 5**. According to the chaotic sequence, mutation units [AUC] at position 2 and [UCG] at position 4 are selected by ($z \oplus w$). If the mutation units selected are the same, the selection will continue according to the subsequent chaotic sequence.

The codons mutated accordingly, as shown in **Figure 6**. The red and green codons convert to each other.

Step 5: RNA decoding rules. Based on chaotic sequence, decoding rules are selected, and binary matrix is obtained. Then convert it into decimal matrix, which is the final ciphertext C.

According to the RNA coding theory, each RNA gene carries certain information of the images. Dynamic RNA encoding rules and RNA decoding rules could increase the randomness of ciphertext and the resistance to statistical attacks. Crossover and mutation based on chaotic sequences could increase the unpredictability of the encryption algorithm. Therefore, a different ciphertext can be obtained by using different crossover and mutation rules and different encoding and decoding rules.

Decryption Scheme

Due to the symmetrical image cryptosystem, the cipher matrix can be decrypted and the original images can be restored using the reverse process of the encryption process, as shown in **Figure 7**. After the reverse mutation and crossover of RNA operation and the reverse scrambling and diffusion of 3D Arnold algorithm, the added random points were removed and the image was decomposed, and three original images could be obtained.

PERFORMANCE ANALYSIS

Simulation Results

In order to verify the performance of the designed cryptosystem, several experiments were carried out on 3D images. The experiments were tested on a computer: Intel Core i7 CPU 2.9GHz, RAM 32 GB. The operating system is Windows 10. The simulation software is Matlab 2016b. Set the parameters as follows: $L = 0.025$, $C = 0.025$, $a_1 = 5.8$, $a_2 = 0.825$, $b_1 = 2$, $b_2 = 10$, and the initial values are (1, 3, 1, −0.7). To test the encryption performance, three 3D images Car (39888×3), Jet (25896×3), and Rocket (51310×3) are used as encryption models. The simulation results of cryptosystem are shown in **Figure 8**. The encrypted images can completely hide the original images, and decryption process can successfully restore the original images with the keys. Based on the characteristics of 3D images, it is considered as a special color image. Therefore, the performance analysis methods of color images cryptosystem can be applied to 3D images encryption.

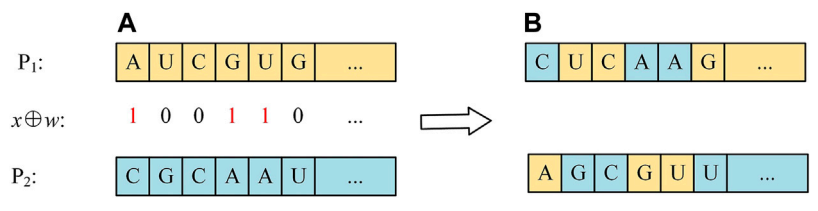

FIGURE 4 | Crossover process. **(A)** Before crossover. **(B)** After crossover.

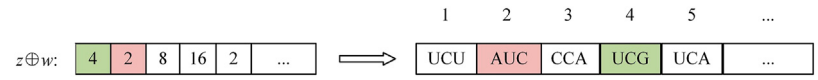

FIGURE 5 | Selection of mutant genomes.

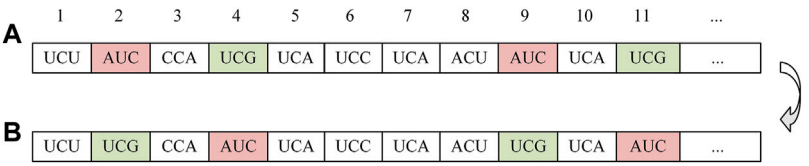

FIGURE 6 | Mutation process. **(A)** Before mutation. **(B)** After mutation.

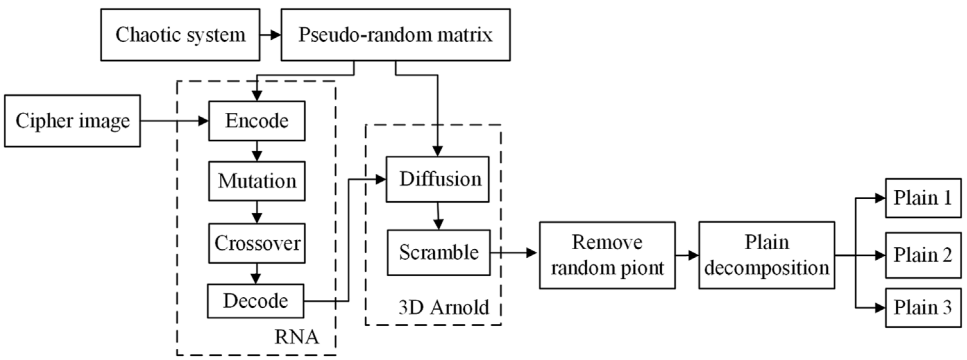

FIGURE 7 | The flowchart of decryption algorithm.

Key Space Analysis

In cryptosystem, the key space must be large enough, which is critical to the encryption algorithm. The secret key consists of 1) system parameters L, C, a_1, a_2, b_1, and b_2; 2) initial value of the chaotic system (x, y, z, w); 3) SHA-256 hash value k_1, k_2, k_3, k_4; and 4) parameter of vertex matrix k_5. With the calculation accuracy of 10^{-15}, the key space will reach 2^{747}, which exceeds the minimum requirement of 2^{100}, and could resist brute force attacks [49]. **Table 4** shows the test results of key space. Compared with other literatures, key space of this cryptosystem is larger.

Key Sensitivity Analysis

Key sensitivity is an important feature of encryption algorithm. An effective cryptosystem should be extremely sensitive to the key. The cipher matrix obtained by encrypting the same plaintext matrix should be significantly different when there is a small change in the key. In the key sensitivity test, a slight change in the key during the decryption results in three restored images that are completely different from originals, as shown in **Figure 9**.

Histogram Analysis

In order to hide the information about vertex coordinates, the ciphertext histograms should be flat and evenly distributed. The histogram results are plotted in **Figure 10**. In the figure, the plaintext and ciphertext histograms are completely different. There is a clear coordinate aggregation interval in the plaintext matrix, while the coordinates in the cipher matrix are uniformly distributed.

Moreover, the χ^2 test results can be used to quantitatively analyze whether vertex coordinates are evenly distributed. In **Table 5**, the χ^2 test results of plaintexts and ciphertexts are presented. The measured results of the proposed algorithm are less than the critical values of different probabilities (10%, 5%, and 1%), indicating that the encryption algorithm could overwrite the statistics of vertex coordinates and resist statistical attacks.

Correlation Analysis

To protect vertex coordinate information, the statistics needs to be hidden, and the correlation between adjacent vertices coordinates needs to be reduced. The relevant equations are given below:

$$\gamma_{xy} = \frac{E\{[x - E(x)] - [y - E(y)]\}}{\sqrt{D(x)D(y)}} \tag{11}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

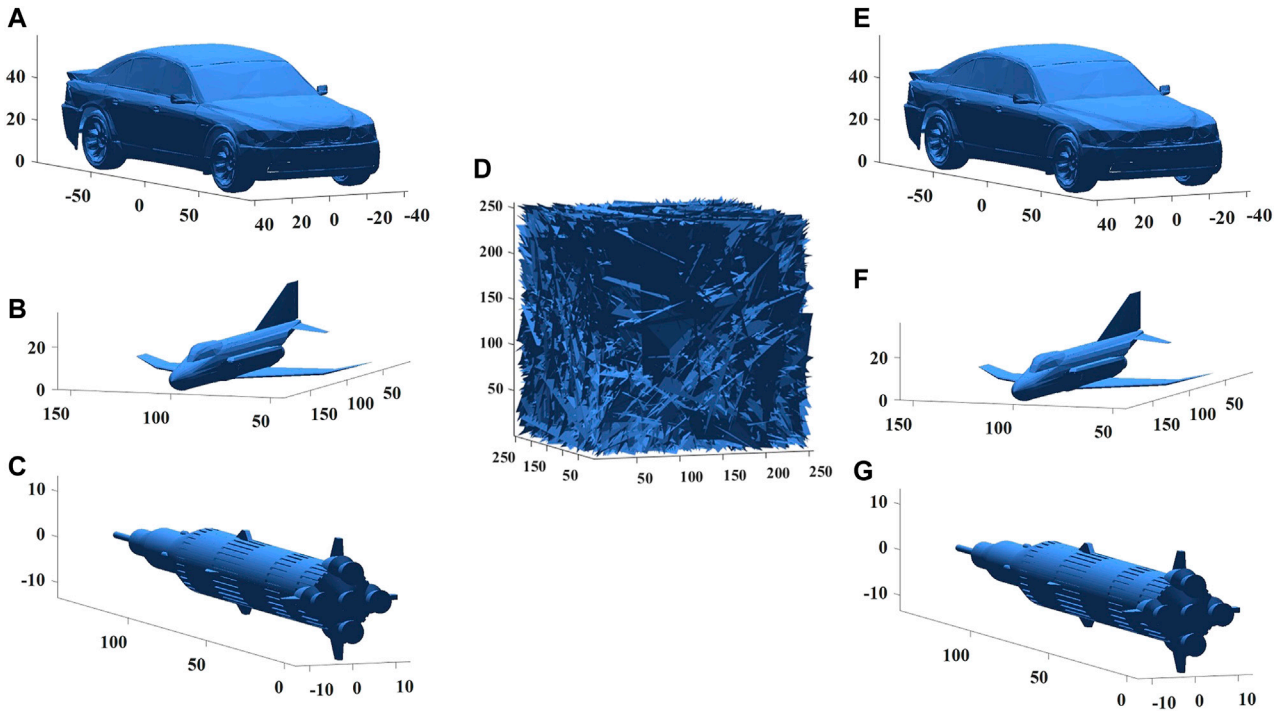

FIGURE 8 | The simulation results. **(A)** Car image. **(B)** Jet image. **(C)** Rocket image. **(D)** Cipher image. **(E)** Decrypted Car image. **(F)** Decrypted Jet image. **(G)** Decrypted Rocket image.

TABLE 4 | Key space for different algorithms

Algorithm	Proposed	Reference [7]	Reference [8]	Reference [38]	Reference [42]	Reference [50]
Key space	2^{747}	2^{599}	2^{240}	2^{280}	2^{256}	2^{224}

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2 \tag{13}$$

Figures 11A,C,E show the correlation of plaintexts; the coordinate distribution is intensive, and the vertex coordinates are highly correlated. On the contrary, **Figures 11B,D,F** demonstrated that the correlation of the encryption model is low, which means that the algorithm could reduce the correlations between adjacent vertices in each direction and resist statistical attacks.

When the absolute value of the correlation coefficient is close to 1, it means that the coordinate values of the large region in the vertex matrix are small. On the contrary, if it is close to 0, the cryptosystem could confuse coordinate positions effectively. The correlation coefficient between adjacent coordinates are shown in **Table 6**. In each direction, the adjacent coordinates of the plaintexts are highly correlated and the correlation between adjacent coordinates of ciphertexts is low.

Randomness Analysis

In order to ensure the uniform distribution of cipher coordinate values, a variety of 3D images are adopted to measure the security of cipher. SP (Special Publications) 800-22 is a randomness standard test published by NIST, which contains 15 sub-tests that identify the randomness of the encryption algorithm. NIST test uses p-value magnitude and the pass rate to reflect the bit sequence randomness property of the encryption algorithm. When the p-value is greater than or equal to 0.01, it is considered that the bit sequence has passed the NIST test, that is, the bit sequence has randomness. The pass rate reflected the number of sample sequences that pass the randomness test.

With different test samples and different initial conditions, several cryptographic matrixes are obtained. Then, the cipher matrix is converted to binary sequence. The value of each cipher matrix is represented by eight bits. Thus, the length of test sample is 86,400,000 bits. The randomness test results are present in **Table 7**, with the worst set of data. The test sample can pass all 15 sub-tests, indicating that the cipher matrix has high randomness.

Information Entropy Analysis

Information entropy is used to measure the average amount of information in the whole image, and its theoretical value is 8. The

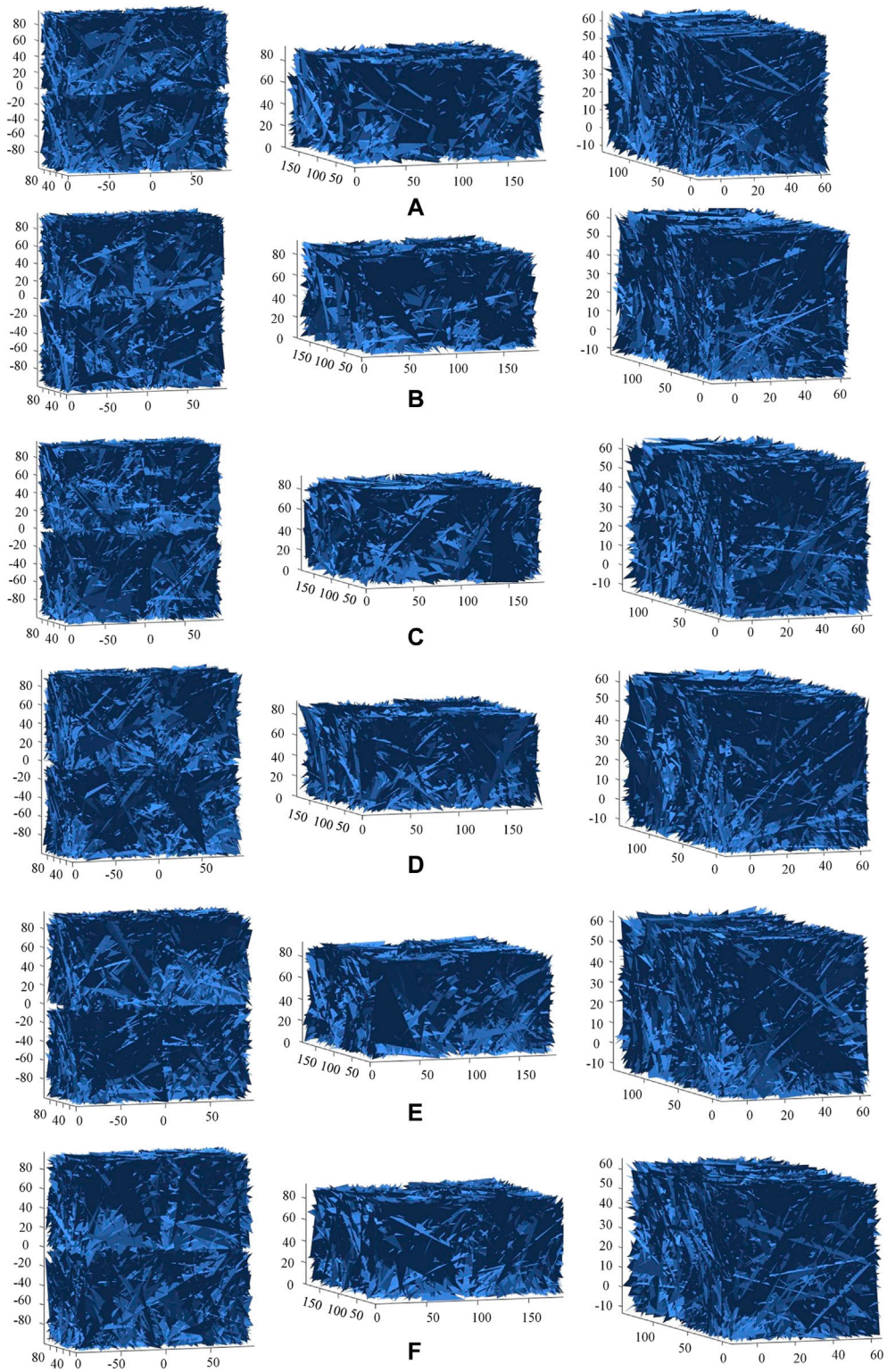

FIGURE 9 | The key sensitivity test. **(A)** a_1+10^{-15}, **(B)** a_2+10^{-15}, **(C)** b_1+10^{-15}, **(D)** b_2+10^{-15}, **(E)** $L+10^{-15}$, **(F)** $C+10^{-15}$.

more evenly coordinate values are distributed, the less effective information the information source has. The coordinates in the vertex matrix are floating-point numbers. Therefore, the positive integer less than or equal to the coordinates in vertex matrix is taken. Thus, for the vertex matrix with 256 levels, information entropy can be expressed as:

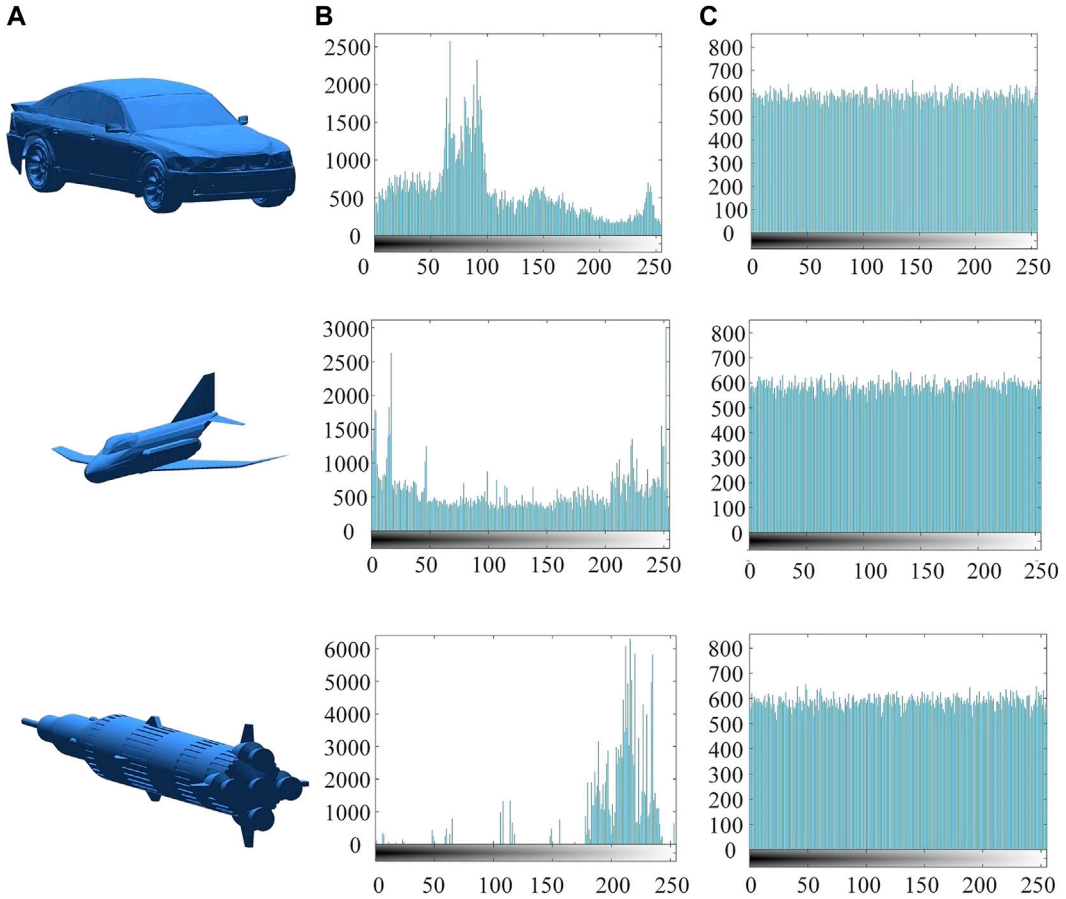

FIGURE 10 | The histogram analysis results. **(A)** Plaintext images. **(B)** Histograms of plaintext images. **(C)** Histograms of cipher images.

TABLE 5 | Results of the χ^2-value test

3D model	χ^2-value (plaintext)	χ^2-value (ciphertext)	Critical value		
			$\chi^2_{0.1}$ (255)	$\chi^2_{0.05}$ (255)	$\chi^2_{0.01}$ (255)
Car	72,638.9132	246.2416	Pass	Pass	Pass
Jet	47,615.5636	260.4825	Pass	Pass	Pass
Rocket	647,556.5317	263.6170	Pass	Pass	Pass

$$H(x) = \sum_{i=0}^{N} p(x_i) \log_2 \frac{1}{p(x_i)} \tag{14}$$

Table 8 gives the information entropy of plaintexts and ciphertexts. The information entropy of original images Car, Jet, and Rocket of different sizes are 7.7123, 7.8348, and 5.929, and the information entropy of ciphertexts are significantly improved to 7.9988, 7.9988, and 7.9987, respectively. The information entropies of ciphertexts are larger than that of the plaintexts and close to the theoretical value. Compared with other algorithms, the proposed algorithm could confuse the coordinate information successfully and resist statistical attacks.

Differential Attack Analysis

When one of the original images is changed in a slight way, the encrypted images should be significantly different. NPCR and UACI could reflect the sensitivity of the original 3D images, as shown in the following formula:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{15}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\% \tag{16}$$

$$D(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, C_1(i,j) = C_2(i,j) \end{cases} \tag{17}$$

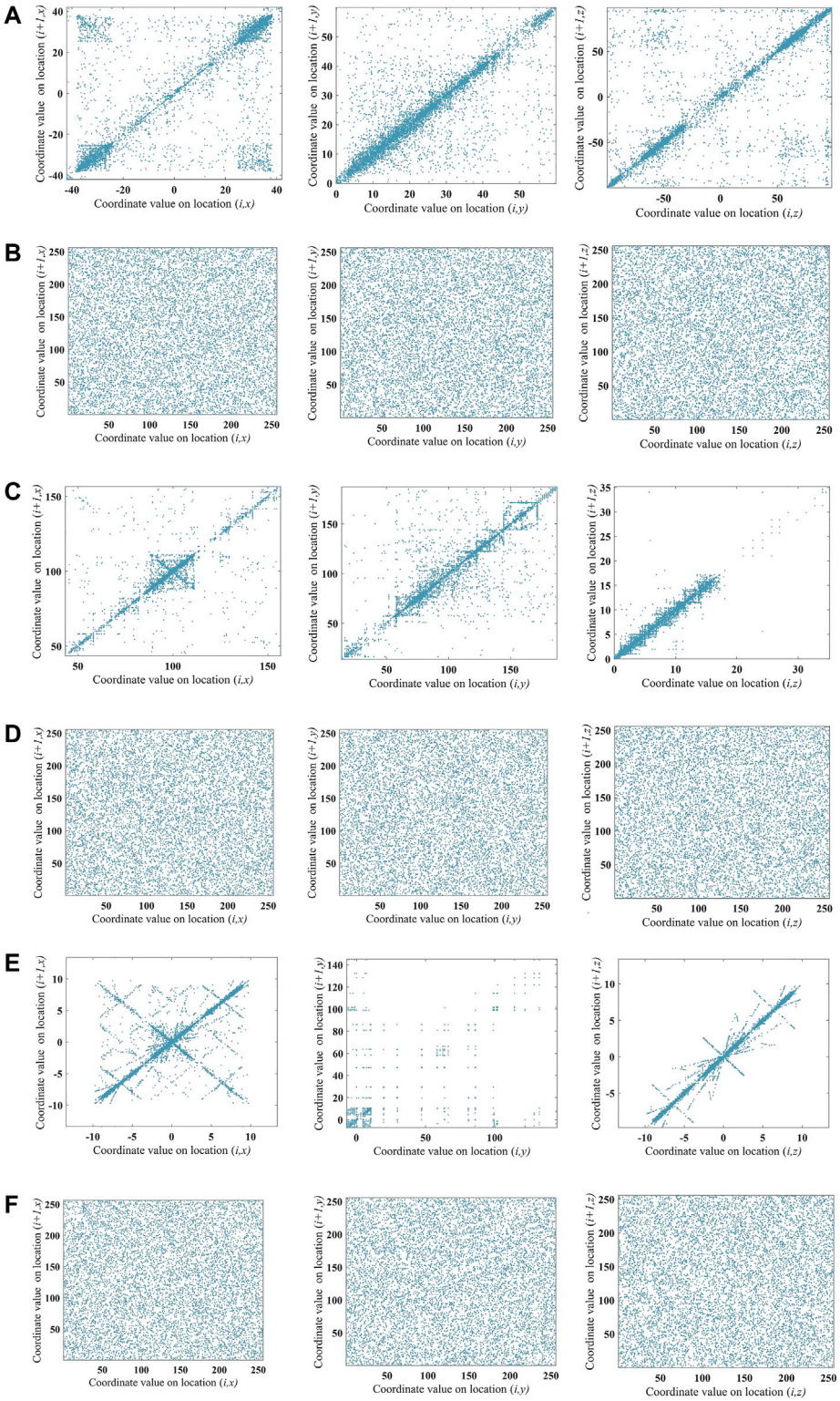

FIGURE 11 | The correlation analysis of different images. **(A)** Car plaintext. **(B)** Car ciphertext. **(C)** Jet plaintext. **(D)** Jet ciphertext. **(E)** Rocket plaintext. **(F)** Rocket ciphertext.

TABLE 6 | The correlation coefficients between the plain images and cipher images

Algorithm	3D image	*X*-direction		*Y*-direction		*Z*-direction	
		Plaintext	Ciphertext	Plaintext	Ciphertext	Plaintext	Ciphertext
Our scheme	Car	0.40657	0.010585	0.24970	0.01920	0.68542	−0.00369
	Jet	0.04589	−0.005583	0.43335	0.00810	0.56907	0.01150
	Rocket	0.72592	−0.010559	0.94497	−0.00540	0.98495	0.00864
Reference [5]	Kun jet	0.9763	0.0118	0.9878	0.0062	0.9869	0.00038
	Air early warming	0.9982	−0.0041	0.9954	0.0051	0.9975	−0.0075
	Boeing-747	0.9794	−0.0030	0.9992	0.0002	0.9815	−0.0004
Reference [8]	Terrain	0.9923	−0.0254	0.7365	−0.0097	0.9850	0.0049

TABLE 7 | NIST test results

Test		p-Value	Pass rate	Result
Frequency	—	0.249284	0.99	Pass
Block frequency	—	0.262249	0.99	Pass
Cumulative sums	Forward	0.978072	0.99	Pass
	Reverse	0.834308	0.99	Pass
Runs	—	0.009535	1	Pass
Longest run	—	0.678686	1	Pass
Binary matrix rank	—	0.319084	1	Pass
FFT	—	0.657933	0.98	Pass
Non-overlapping template matching	—	0.153763	0.97	Pass
Overlapping template matching	—	0.058984	0.96	Pass
Maurer's "universal statistical"	—	0.304126	0.99	Pass
Approximate entropy	—	0.534146	0.99	Pass
The random excursions	$x = -4$	0.378138	0.98	Pass
	$x = -3$	0.299251	1	Pass
	$x = -2$	0.350485	1	Pass
	$x = -1$	0.637119	1	Pass
	$x = 1$	0.299251	1	Pass
	$x = 2$	0.350485	0.98	Pass
	$x = 3$	0.888137	1	Pass
	$x = 4$	0.772760	0.97	Pass
Random excursions variant	$x = -9$	0.534146	1	Pass
	$x = -8$	0.213309	0.95	Pass
	$x = -7$	0.232760	0.95	Pass
	$x = -6$	0.378138	0.97	Pass
	$x = -5$	0.888137	0.95	Pass
	$x = -4$	0.637119	1	Pass
	$x = -3$	0.060239	0.98	Pass
	$x = -2$	0.949602	1	Pass
	$x = -1$	0.637119	1	Pass
	$x = 1$	0.253551	1	Pass
	$x = 2$	0.407091	0.98	Pass
	$x = 3$	0.162606	0.97	Pass
	$x = 4$	0.437274	1	Pass
	$x = 5$	0.437274	1	Pass
	$x = 6$	0.407091	1	Pass
	$x = 7$	0.949602	0.98	Pass
	$x = 8$	0.995711	0.98	Pass
	$x = 9$	0.964295	0.98	Pass
Serial	$p\text{-Value}_1$	0.595549	0.99	Pass
	$p\text{-Value}_2$	0.035174	0.99	Pass
Linear complexity	—	0.162606	1	Pass

where C_1 and C_2 represent ciphertexts before and after a coordinate value of plaintext changes by 1. When the NPCR is close to 1 and the UACI is about 0.3346, the algorithm is considered to have passed the test.

The idea values of NPCR and UACI are given [51, 52]. According to **Table 9** and **Table 10**, the mean value of NPCR and UACI of the three images is 99.6154% and 33.35%. **Figure 12** shows the NPCR and UACI calculated by randomly varying the vertex matrix values in different test model. The test results of NPCR and UACI are greater than the theoretical values with a confidence level of 0.05. A comparison of NPCR and UACI with different algorithms

TABLE 8 | The information entropy test for different algorithms

3D model	Proposed scheme				Reference [3]		Reference [8]	Reference [28]	Reference [29]
	Car	Jet	Rocket	Lena	Baboon	Peppers	Terrain	Camera	Camera
Plaintext	7.7123	7.8348	5.929	7.2544	7.6599	7.2118	6.8030	7.0097	7.0097
Ciphertext	7.9988	7.9988	7.9987	7.9959	7.9959	7.9959	7.9980	7.9968	7.9972

TABLE 9 | The NPCR results for different images

3D image	NPCR (%)	Text result		
		$NPCR^*_{0.05}$ = 99.5693%	$NPCR^*_{0.01}$ = 99.5527%	$NPCR^*_{0.001}$ = 99.5341%
Car	99.6197	Pass	Pass	Pass
Jet	99.6147	Pass	Pass	Pass
Rocket	99.6119	Pass	Pass	Pass

TABLE 10 | The UACI results for different images

3D image	UACI (%)	Text result		
		$UACI^{*+}_{0.05}$ = 33.6447% $UACI^{*-}_{0.05}$ = 33.2824%	$UACI^{*+}_{0.01}$ = 33.7016% $UACI^{*-}_{0.01}$ = 33.2255%	$UACI^{*+}_{0.001}$ = 33.7677% $UACI^{*-}_{0.001}$ = 33.1594%
Car	33.3857	Pass	Pass	Pass
Jet	33.3774	Pass	Pass	Pass
Rocket	33.2855	Pass	Pass	Pass

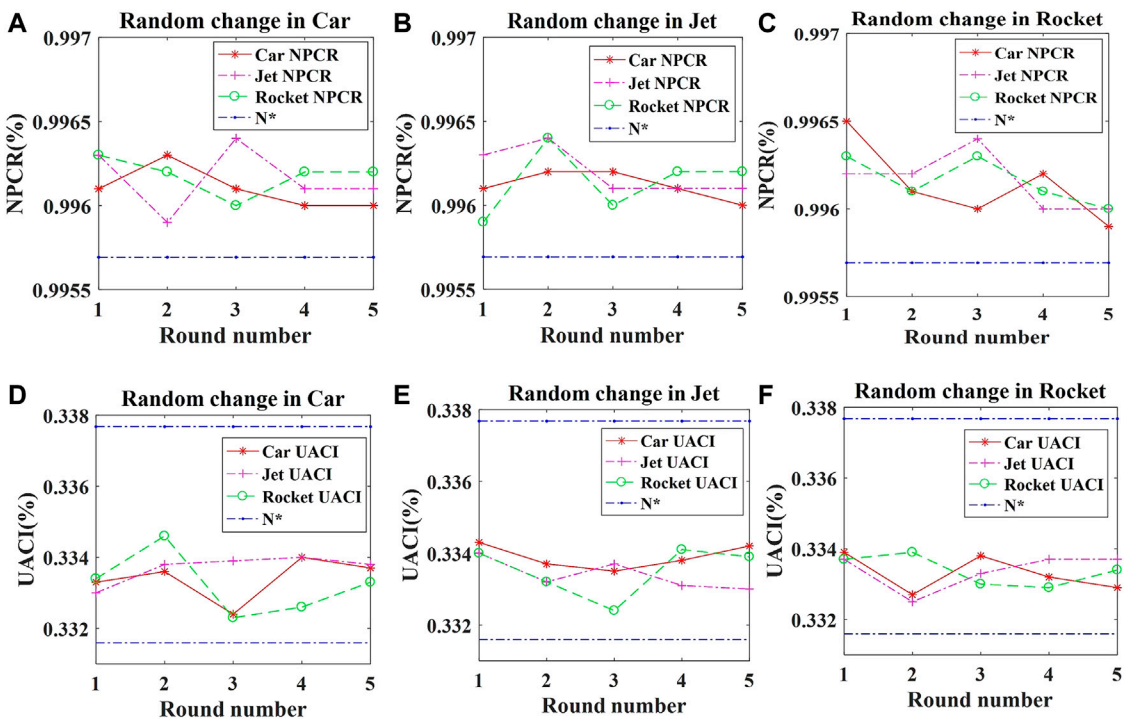

FIGURE 12 | The test results of differential attacks. **(A)** NPCR of Car change. **(B)** NPCR of Jet change. **(C)** NPCR of Rocket change. **(D)** UACI of Car change. **(E)** UACI of Jet change. **(F)** UACI of Rocket change.

TABLE 11 | Comparison of NPCR and UACI with different algorithms

Algorithm	Proposed scheme	Reference [5]	Reference [8]	Reference [28]	Reference [29]	Reference [36]	Reference [43]
NPCR (%)	99.6197	99.61	99.59	99.54	99.60	99.6060	99.6114
UACI (%)	33.3857	33.44	33.26	32.19	33.45	33.5126	33.54

is shown in **Table 11**, which proves the ability to resist differential attack.

Time Analysis

The image cryptosystem mainly includes three processes: chaotic system iteration, 3D Arnold algorithm and DNA encryption. The encryption time of images with 348,282 vertex coordinates is 30.1795 s. In Ref. [36], the encryption time of 89,271 data is 0.261795 s. In Ref. [40], the encryption time of the 256 × 256 gray image is 7.59 s. The proposed cryptosystem sacrifices the encryption time to ensure the encryption effect.

CONCLUSION

A novel 3D image encryption based on the memristive chaotic system and RNA crossover and mutation is proposed. Firstly, the chaotic system based on two memristors is analyzed by bifurcation diagrams and Lyapunov exponential spectrums. It is shown that the chaotic system has complex dynamical behaviors and large parameter space, which are suitable for image encryption. Secondly, the initial values are generated by SHA-256, so different plaintexts and merge orders will generate different keys and chaotic sequences. Besides, an improved 3D Arnold algorithm is used to confuse the vertex positions and convert coordinates. Based on dynamic RNA encoding and decoding rules, the RNA crossover and mutation algorithms are given to directly exchange codons. In addition, the cryptosystem can encrypt multiple images at the same time, which improves security and effectiveness. Finally, experimental results indicate that the cryptosystem could ensure the security of three 3D images simultaneously, and the security analysis verifies that it could resist various attacks effectively.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

RC provided the idea of algorithm, carried out the simulations, arranged the architecture and drafted the manuscript. SZ and XG supervised the work and revised the manuscript. Both authors read and approved the final manuscript.

FUNDING

This research was funded by the National Natural Science Foundation of China (No. 61231006 and No. 61501078).

REFERENCES

1. Jiang R, Zhou H, Zhang W, Yu N. Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models. *IEEE Trans Multimedia* (2018) 20(1):55–67. doi:10.1109/tmm.2017.2723244
2. Peng Y, He S, Sun K. A Higher Dimensional Chaotic Map with Discrete Memristor. *AEU - Int J Elect Commun* (2021) 129:153539–7. doi:10.1016/j.aeue.2020.153539
3. Joshi AB, Kumar D, Gaffar A, Mishra DC. Triple Color Image Encryption Based on 2D Multiple Parameter Fractional Discrete Fourier Transform and 3D Arnold Transform. *Opt Lasers Eng* (2020) 133:106139–13. doi:10.1016/j.optlaseng.2020.106139
4. Pham G, Lee S-H, Kwon K-R. Interpolating Spline Curve-Based Perceptual Encryption for 3D Printing Models. *Appl Sci* (2018) 8(2):242–54. doi:10.3390/app8020242
5. Xu J, Zhao C, Mou J. A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation. *IEEE Access* (2020) 8(99):145995–6005. doi:10.1109/access.2020.3005925
6. Pham N-G, Lee S-H, Lee S-H, Kwon O-H, Kwon K-R. 3D Printing Model Random Encryption Based on Geometric Transformation. *Int J Machine Learn Comput* (2018) 8(2):186–90. doi:10.18178/ijmlc.2018.8.2.685
7. Jin X, Zhu S, Xiao C, Sun H, Li X, Zhao G, et al. 3D Textured Model Encryption *via* 3D Lu Chaotic Mapping. *Sci China Inf Sci* (2017) 60(12):1–9. doi:10.1007/s11432-017-9266-1
8. Wang X, Xu M, Li Y. Fast Encryption Scheme for 3D Models Based on Chaos System. *Multimed Tools Appl* (2019) 78(23):33865–84. doi:10.1007/s11042-019-08171-2
9. An X, Qiao S. The Hidden, Period-Adding, Mixed-Mode Oscillations and Control in a HR Neuron under Electromagnetic Induction. *Chaos, Solitons & Fractals* (2021) 143:110587–18. doi:10.1016/j.chaos.2020.110587
10. Qiao S, An X-L. Dynamic Expression of a HR Neuron Model under an Electric Field. *Int J Mod Phys B* (2020) 35(02):2150024–3. doi:10.1142/s0217979221500247
11. Ma X, Mou J, Liu J, Ma C, Yang F, Zhao X. A Novel Simple Chaotic Circuit Based on Memristor-Memcapacitor. *Nonlinear Dyn* (2020) 100(3):2859–76. doi:10.1007/s11071-020-05601-x
12. Yu F, Shen H, Zhang Z, Huang Y, Cai S, Du S. Dynamics Analysis, Hardware Implementation and Engineering Applications of Novel Multi-Style Attractors in a Neural Network under Electromagnetic Radiation. *Chaos, Solitons & Fractals* (2021) 152:111350–14. doi:10.1016/j.chaos.2021.111350
13. Yu F, Zhang Z, Shen H, Huang Y, Cai S, Jin J, et al. Design and FPGA Implementation of a Pseudo-random Number Generator Based on a Hopfield Neural Network under Electromagnetic Radiation. *Front Phys* (2021) 9:1–15. doi:10.3389/fphy.2021.690651
14. Ma C, Mou J, Xiong L, Banerjee S, Liu T, Han X. Dynamical Analysis of a New Chaotic System: Asymmetric Multistability, Offset Boosting Control and Circuit Realization. *Nonlinear Dyn* (2021) 103(3):2867–80. doi:10.1007/s11071-021-06276-8
15. Liu T, Yan H, Banerjee S, Mou J. A Fractional-Order Chaotic System with Hidden Attractor and Self-Excited Attractor and its DSP Implementation. *Chaos, Solitons & Fractals* (2021) 145(2):110791–12. doi:10.1016/j.chaos.2021.110791

16. Liu T, Banerjee S, Yan H, Mou J. Dynamical Analysis of the Improper Fractional-Order 2D-SCLMM and its DSP Implementation. *Eur Phys J Plus* (2021) 136(5):1–17. doi:10.1140/epjp/s13360-021-01503-y
17. Liu H, Zhang Y, Kadir A, Xu Y. Image Encryption Using Complex Hyper Chaotic System by Injecting Impulse into Parameters. *Appl Maths Comput* (2019) 360:83–93. doi:10.1016/j.amc.2019.04.078
18. Liu H, Kadir A, Liu J. Color Pathological Image Encryption Algorithm Using Arithmetic over Galois Field and Coupled Hyper Chaotic System. *Opt Lasers Eng* (2019) 122:123–33. doi:10.1016/j.optlaseng.2019.05.027
19. Liu H, Kadir A, Xu C. Cryptanalysis and Constructing S-Box Based on Chaotic Map and Backtracking. *Appl Maths Comput* (2020) 376:125153. doi:10.1016/j.amc.2020.125153
20. Liu H, Kadir A, Xu C. Color Image Encryption with Cipher Feedback and Coupling Chaotic Map. *Int J Bifurcation Chaos* (2020) 30(12):2050173. doi:10.1142/s0218127420501734
21. Si Y, Liu H, Chen Y. Constructing Keyed strong S-Box Using an Enhanced Quadratic Map. *Int J Bifurcation Chaos* (2021) 31(10):2150146. doi:10.1142/s0218127421501467
22. Liu H, Wang X, Kadir A. Constructing Chaos-Based Hash Function *via* Parallel Impulse Perturbation. *Soft Comput* (2021) 25(16):11077–86. doi:10.1007/s00500-021-05849-4
23. Ma C, Mou J, Li P, Liu T. Dynamic Analysis of a New Two-Dimensional Map in Three Forms: Integer-Order, Fractional-Order and Improper Fractional-Order. *Eur Phys J Spec Top* (2021) 230(7-8):1945–57. doi:10.1140/epjs/s11734-021-00133-w
24. Yu F, Li L, He B, Liu L, Qian S, Zhang Z, et al. Pseudorandom Number Generator Based on a 5D Hyperchaotic Four-wing Memristive System and its FPGA Implementation. *Eur Phys J Spec Top* (2021) 230(7-8):1763–72. doi:10.1140/epjs/s11734-021-00132-x
25. Peng Y, He S, Sun K. Chaos in the Discrete Memristor-Based System with Fractional-Order Difference. *Results Phys* (2021) 24:104106–7. doi:10.1016/j.rinp.2021.104106
26. Chen X, Qian S, Yu F, Zhang Z, Shen H, Huang Y, et al. Pseudorandom Number Generator Based on Three Kinds of Four-Wing Memristive Hyperchaotic System and its Application in Image Encryption. *Complexity* (2020) 2020:1–17. doi:10.1155/2020/8274685
27. Ma X, Mou J, Xiong L, Banerjee S, Cao Y, Wang J. A Novel Chaotic Circuit with Coexistence of Multiple Attractors and State Transition Based on Two Memristors. *Chaos, Solitons & Fractals* (2021) 152:111363–11. doi:10.1016/j.chaos.2021.111363
28. Yang F, Mou J, Ma C, Cao Y. Dynamic Analysis of an Improper Fractional-Order Laser Chaotic System and its Image Encryption Application. *Opt Lasers Eng* (2020) 129:106031–16. doi:10.1016/j.optlaseng.2020.106031
29. Li X, Mou J, Xiong L, Wang Z, Xu J. Fractional-order Double-Ring Erbium-Doped Fiber Laser Chaotic System and its Application on Image Encryption. *Opt Laser Tech* (2021) 140:107074–18. doi:10.1016/j.optlastec.2021.107074
30. Yu F, Shen H, Zhang Z, Huang Y, Cai S, Du S. A New Multi-Scroll Chua's Circuit with Composite Hyperbolic tangent-cubic Nonlinearity: Complex Dynamics, Hardware Implementation and Image Encryption Application. *Integration* (2021) 81:71–83. doi:10.1016/j.vlsi.2021.05.011
31. Yu F, Zhang Z, Shen H, Huang Y, Cai S, Du S. FPGA Implementation and Image Encryption Application of a New PRNG Based on a Memristive Hopfield Neural Network with a Special Activation Gradient. *Chin Phys. B* (2021) 31(2):20505–020505. doi:10.1088/1674-1056/ac3cb2
32. Mou J, Yang F, Chu R, Cao Y. Image Compression and Encryption Algorithm Based on Hyper-Chaotic Map. *Mobile Netw Appl* (2019) 26(5):1849–61. doi:10.1007/s11036-019-01293-9
33. Yang F, Mou J, Luo C, Cao Y. An Improved Color Image Encryption Scheme and Cryptanalysis Based on a Hyperchaotic Sequence. *Phys Scr* (2019) 94(8):085206–9. doi:10.1088/1402-4896/ab0033
34. Ravichandran D, Praveenkumar P, Balaguru Rayappan JB, Amirtharajan R. Chaos Based Crossover and Mutation for Securing DICOM Image. *Comput Biol Med* (2016) 72:170–84. doi:10.1016/j.compbiomed.2016.03.020
35. Chai X, Bi J, Gan Z, Liu X, Zhang Y, Chen Y. Color Image Compression and Encryption Scheme Based on Compressive Sensing and Double Random Encryption Strategy. *Signal Process.* (2020) 176:107684–18. doi:10.1016/j.sigpro.2020.107684
36. Zhang X, Hu Y. Multiple-image Encryption Algorithm Based on the 3D Scrambling Model and Dynamic DNA Coding. *Opt Laser Tech* (2021) 141(441):107073–16. doi:10.1016/j.optlastec.2021.107073
37. Chai X, Chen Y, Broyde LA Novel Chaos-Based Image Encryption Algorithm Using DNA Sequence Operations. *Opt Lasers Eng* (2017) 88:197–213. (Complete). doi:10.1016/j.optlaseng.2016.08.009
38. Chai X, Fu X, Gan Z, Lu Y, Chen Y. A Color Image Cryptosystem Based on Dynamic DNA Encryption and Chaos. *Signal Process.* (2019) 155(FEB.):44–62. doi:10.1016/j.sigpro.2018.09.029
39. Wang X-Y, Zhang Y-Q, Zhao Y-Y. A Novel Image Encryption Scheme Based on 2-D Logistic Map and DNA Sequence Operations. *Nonlinear Dyn* (2015) 82(3):1269–80. doi:10.1007/s11071-015-2234-7
40. Chai X, Gan Z, Lu Y, Chen Y, Han D. A Novel Image Encryption Algorithm Based on the Chaotic System and DNA Computing. *Int J Mod Phys C* (2017) 28(05):1750069–24. doi:10.1142/S0129183117500693
41. Hao J, Li H, Yan H, Mou J. A New Fractional Chaotic System and its Application in Image Encryption with DNA Mutation. *IEEE Access* (2021) 9:52364–77. doi:10.1109/ACCESS.2021.3069977
42. Martín del Rey A. A Method to Encrypt $$3$$ 3 D Solid Objects Based on Three-Dimensional Cellular Automata. In: E Onieva, I Santos, E Osaba, H Quintián, E Corchado, editors. *Lecture Notes in Computer Science*, 9121. Cham: Springer (2015). p. 427–38. doi:10.1007/978-3-319-19644-2_36
43. Devi RS, Aravind ARN, Vishal JC, Amritha D, Thenmozhi K, Rayappan JBB, et al. Image Encryption through RNA Approach Assisted with Neural Key Sequences. *Multimed Tools Appl* (2020) 79(17-18):12093–124. doi:10.1007/s11042-019-08562-5
44. Wang X, Liu L. Application of Chaotic Josephus Scrambling and RNA Computing in Image Encryption. *Multimed Tools Appl* (2021) 80(15):23337–58. doi:10.1007/s11042-020-10209-9
45. Wang X, Guan N. A Novel Chaotic Image Encryption Algorithm Based on Extended Zigzag Confusion and RNA Operation. *Opt Laser Tech* (2020) 131(6):106366–17. doi:10.1016/j.optlastec.2020.106366
46. Abbasi AA, Mazinani M, Hosseini R. Chaotic Evolutionary-Based Image Encryption Using RNA Codons and Amino Acid Truth Table. *Opt Laser Tech* (2020) 132(12):106465–13. doi:10.1016/j.optlastec.2020.106465
47. JarJar A. Two Advanced Classics Exploiting DNA and RNA Characteristics to Encrypt a Color Image. *Multimed Tools Appl* (2021) 80(16):24603–29. doi:10.1007/s11042-021-10658-w
48. Zhang D, Chen L, Li T. Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation. *Entropy* (2021) 23(3):361–23. doi:10.3390/e23030361
49. Zhu C, Gan Z, Lu Y, Chai X. An Image Encryption Algorithm Based on 3-D DNA Level Permutation and Substitution Scheme. *Multimed Tools Appl* (2019) 79(11-12):7227–58. doi:10.1007/s11042-019-08226-4
50. Jin X, Wu Z, Song C, Zhang C, Li X. 3D Point Cloud Encryption through Chaotic Mapping. In: *Pacific Rim Conference on Multimedia*, 9916 (2016). p. 119–29. doi:10.1007/978-3-319-48890-5_12
51. Hua Z, Zhou Y, Huang H. Cosine-transform-based Chaotic System for Image Encryption. *Inf Sci* (2019) 480:403–19. doi:10.1016/j.ins.2018.12.048
52. Gao X, Mou J, Xiong L, Sha Y, Yan H, Cao Y. A Fast and Efficient Multiple Images Encryption Based on Single-Channel Encryption and Chaotic System. *Nonlinear Dyn* (2022). doi:10.1007/s11071-021-07192-7

Conflict of Interest: XG was employed by the company Tokai Carbon Dalian Co., Ltd.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

The handling editor declared a shared affiliation with one of the authors RC at time of review.