IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 20, 2020, accepted June 15, 2020, date of publication June 30, 2020, date of current version August 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005925

A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation

JI XU[1], CHEN ZHAO[1,2], AND JUN MOU[1,2]

[1]School of Engineering Practice and Innovation-Entrepreneurship Education, Dalian Polytechnic University, Dalian 116000, China
[2]School of Information Science and Engineering, Dalian Polytechnic University, Dalian 116000, China

Corresponding author: Chen Zhao (zhaochen989@163.com)

This work was supported by the Natural Science Foundation of Liaoning Province under Grant 2020-MS-274.

ABSTRACT In this paper, a novel 3D image file encryption algorithm based on a new discrete chaotic system is presented. Chaotic characteristics of the novel chaotic system are analyzed by phase diagram, Lyapunov exponent, bifurcation diagram. Based on the analysis results, an encryption scheme is designed for 3D image file. The hash value which is calculated from the SHA-256 hash function is used to change the initial condition of the discrete system firstly. And then, the chaotic sequences are used to scramble and spread coordinate value for 3D image file by Arnold matrix and DNA diffusion algorithm. The security analysis shows that the proposed 3D image file encryption algorithm possesses higher security features to preserve the subject and resist conventional attack. The results of this paper give a different application scheme of the 3D image encryption algorithm.

INDEX TERMS 3D image, discrete chaotic system, DNA encryption, Arnold matrix.

I. INTRODUCTION

Advances of the multimedia computing technology and the size of network have unlocked the path for the application of 3D technology. Specially, the rapid prototyping technology has become popular in the industry, medical and military areas [1]–[3]. Currently, the STL (Stereolithography) format is the most popular file format in the rapid prototyping. Based on the advantage of STL language, many custom products can be designed by computer aided design software [4]–[6]. Meanwhile, with the rapid development of internet technology and wireless network, more 3D model files are generated and transformed in internet space.

Although, like another side of the coin, the 3D model file is holding the possibility of unauthorized access and it has a series of intellectual property issues. Therefore, the 3D model file protection has become a great deal of increasing interesting for information security research [7], [8]. Unlike the traditional text message, the 3D model file can be considered as a special image in the computer-aided design software. Moreover, the 3D model file has massive data capacity and more complex spatial distribution. Therefore, the ability of traditional encryption technology such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are suitable for protect multimedia file is question [9]–[11]. This situation makes necessary to improve the encryption ability of existing encryption algorithm.

Chaotic phenomenon is complex behavior in the natural system. It has many significant features such as the highly sensitive of the initial condition and ergodicity. Therefore, these properties can satisfy the requirement of encryption algorithm [12]–[14]. In recent researches, many encryption algorithms based on the chaotic system have proposed [15]–[17]. For example, in the digital image security area, DNA theory is combined with the chaotic system to diffuse the value of the image matrix [18]–[21]. Moreover, in compressive sensing operation, the chaotic sequences are used to build the measured matrix for encrypted image [22]–[26].

So far, there are few encryption algorithms specifically designed for 3D image. On the other side, existing encryption algorithm of 3D image has weakness. In Ref [27], the encryption algorithm is adapted the double round encryption flow. However, the randomness of the pseudo-random number generator algorithm is poor. It cannot longer meet the encryption requirements. Ref [7], [8], [28], [29] using the chaotic system to encrypted the vertex information of 3D object. But these algorithms have drawbacks. Firstly, the key space of

The associate editor coordinating the review of this manuscript and approving it for publication was Shenghong Li.

Ref [28], [29] is small and the performance of resist brute force attack is weak. Secondly, the dynamic behavior of chaotic system in Ref [8], [28] is not complicated. Besides, the encryption algorithms of Ref [7], [8], [29] only have the diffusion part and no scramble operation. That means the cipher model can easily recover by rebuilding the order of the 3D model. Hence, designing a new encryption schemes for the 3D image files becomes a new direction of the cryptosystem.

Generally, the discrete chaotic system has a simple structure, the calculation cost is very small. It can quickly generated a random sequence in the computer system. However, the chaotic behavior of some discrete chaotic system is not complicated. These chaotic systems can‘t satisfy the request for data encryption of multimedia file. Therefore, these discrete chaotic system needs to transform for achieved high randomness. The Cosine Transform Based on the Chaotic System (CTBCS) has complicated chaotic behavior and can generate more complex randomness sequence [30]. Besides, the transform method include two chaotic systems. The system dimension and the number of system parameter has not limited.

Therefore, in this work, a novel 3D image encryption scheme based on the new discrete chaotic system is designed. The encryption algorithm uses the CTBCS system to encrypt the 3D image by Arnold matrix and DNA encryption algorithm. Moreover, the Arnold matrix in this algorithm can diffuse the value of vertex matrix and disorder the arrangement at the same time. Compare with one-dimension chaotic system in the Ref [30], the CTBCS system chooses two high-dimension discrete chaotic systems as a seed system. As one seed system of CTBCS, the quantum logistic system is a kind of 3D-dimension discrete chaotic system. It construed by classical logistic model and has complex dynamical behavior and high-sensitivity of initial condition [31]–[33]. Moreover, in the image encryption area, numerous research objects provide the feasibility in multimedia encryption algorithm [32], [34]–[37].

The rest parts of this paper structure as follow. The dynamic analyses of a novel chaotic system are carried out in Sec. 2. The detail of encryption algorithm and decryption workflow is described in Sec. 3. The results of relevant security performance indexes are presented in Sec. 4. In Sec. 5, obtain important conclusion. conclusion.

II. THE CHAOTIC PROPERTIES OF SEED DISCRETE CHAOTIC SYSTEM

A. THE CHAOTIC BEHAVIOR ANALYSIS OF CTBCS SYSTEM

At the start of this subsection, the detail of CTBCS system is illustrated. The CTBCS (Cosine Transform Based on Chaotic System) is a pathway to improve the randomness for an existing discrete chaotic system. The new discrete system can generate more complex chaotic sequence. The mathematical structure of CTBCS is present as Eq. (3)

$$x_{i+1} = cos(\pi F(a, x_i) + G(b, x_i) + \beta). \tag{1}$$

According to the mathematical structure of CTBCS, $F(a, x_i)$ and $F(b, x_i)$ is seed system from existing chaotic system. a and b are their control parameters. The variable β is a shifting constant.

Based on the theory from Ref [30], the seed system can be any existing chaotic system. Therefore, This chaotic system is construed by two existing high-dimension discrete system. The quantum logistic system and the 3D-SIMM discrete chaotic system. Therefore, the mathematical description of CTBCS as Eq. (2)

$$\begin{cases} x_{i+1} = cos[\pi(r_1 F(x_i) + (1 - r_1)G(x_i)) - b_1] \\ y_{i+1} = cos[\pi(r_1 F(y_i) + (1 - r_1)G(y_i)) - b_1] \\ z_{i+1} = cos[\pi(r_1 F(z_i) + (1 - r_1)G(z_i)) - b_1]. \end{cases} \tag{2}$$

where $F(x_i)$ is the quantum logistic system, $G(x_i)$ is the 3D-SIMM discrete chaotic system. Set $r_1 = -10$ and $1 - r_1 = 11$.

Because of the dissipation parameter β is introduced in the classical logistic system. The quantum logistic system could be described as Eq. (3).

$$F = \begin{cases} x_{i+1} = r(x_i - |x_i|^2) - ry_i \\ y_{i+1} = \mathrm{e}^{-b} \cdot r((2 - x_i - \dot{x}_i)y_i - x_i\dot{z}_i - \dot{x}_i z_i) \\ y_{i+1} = -y_i \cdot \mathrm{e}^{-2b} + y_{i+1} \\ z_{i+1} = \mathrm{e}^{-b} \cdot r(2(1 - \dot{x}_i z_i)z_i - 2x_i y_i - x_i) \\ z_{i+1} = -z_i \cdot \mathrm{e}^{-2b} + z_{i+1}. \end{cases} \tag{3}$$

The Fig 1 (a) is demonstrated the phase diagram of this chaotic system. It obtained by the system parameteres $\gamma = 3.99$, $\beta = 30$ and the initial conditions $(x_0, y_0, z_0) =$ (0.463442265, 0.04532285, 0.002136285). Besides, setting $\Delta = 0.0025$, the Lyapunov exponents [LE_1, LE_2, LE_3]=[0.6370,-27.7477,28.8228]. Moreover, the result of the dimension is 1.0231. Therefore, the result of Lyapunov exponent illustrated that this situation of system can observe the chaotic behavior. The LEs shown in Fig 1 (b) with $\gamma \in$ [3,3.99]. The bifurcation diagram of this system variable x is demonstrated in Fig 1 (c).

The 3D-SIMM discrete chaotic system could be described as Eq. (4). Derived from sine map and ICMIC, the 3D-SIMM system is obtained based on a close-loop modulation coupling pattern [16].

$$G = \begin{cases} x_{i+1} = sin(b_2 z_i) \cdot sin(\frac{c}{x_i}) \\ y_{i+1} = sin(b_2 x_{i+1}) \cdot sin(\frac{c}{y_i}) \\ z_{i+1} = sin(b_2 y_{i+1}) \cdot sin(\frac{c}{z_i}). \end{cases} \tag{4}$$

When the system parameters $a = 1, b_2 = 2\pi, c = 11.5$, initial value $(x_0, y_0, z_0) =$ [0.3,0.5,0.6], the system phase diagram is shown in Fig 1 (d). The Lyapunov exponent of the system is (LE_1, LE_2, LE_3) = (5.2325,4.2972,2.7538). The Lyapunov exponent spectrum and bifurcation diagram are shown in Fig 1 (e) and (f). As shown in Fig 1(e) and (f), 3D-SIMM is hyper-chaotic in total range when a $\in$ [0.33,5].

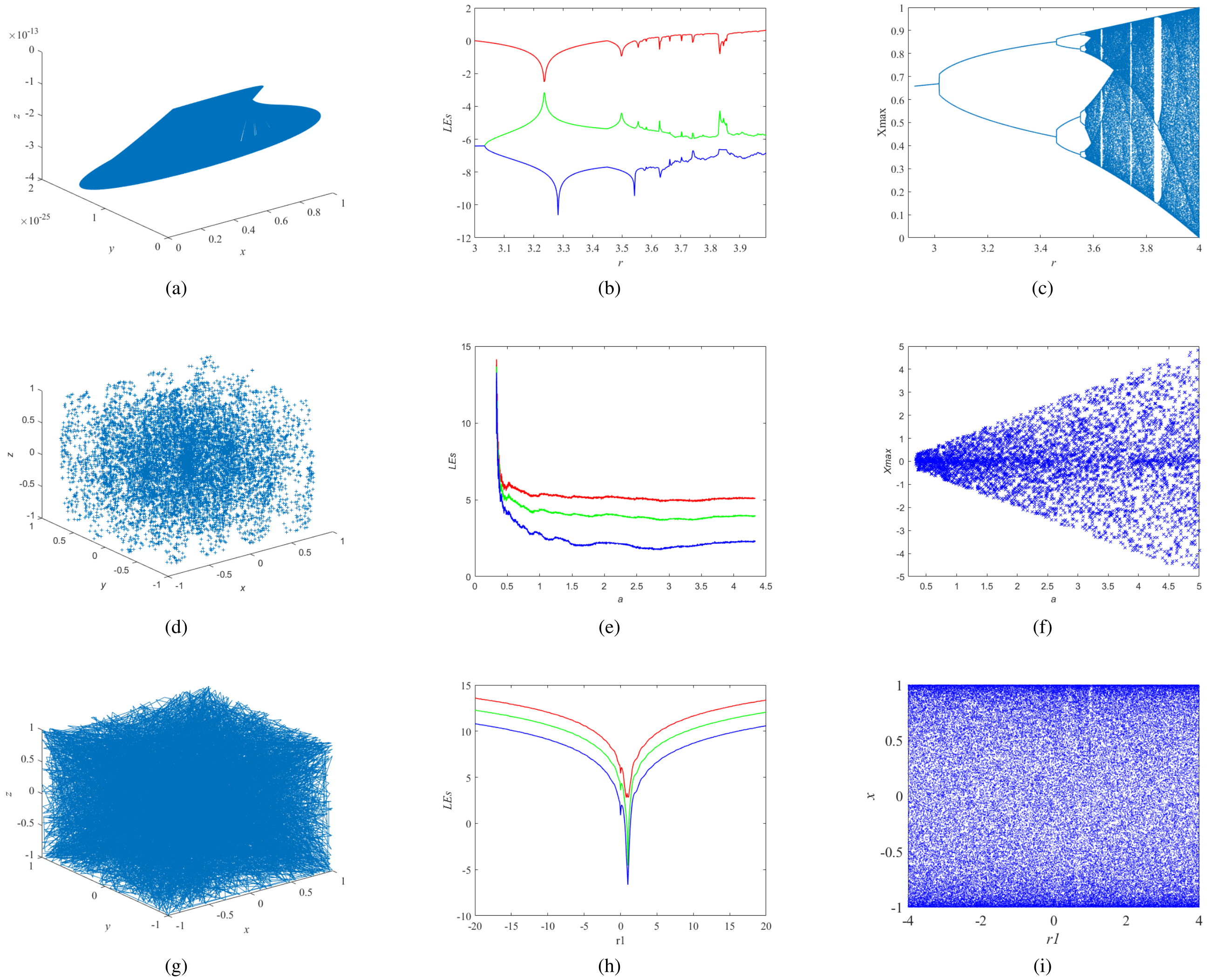


FIGURE 1. The chaotic behavior analyse result: (a) Phase diagram of quantum logistic system (b) Lyapunov spectrum of quantum logistic system (c) Bifurcation diagram of quantum logistic system (d) Phase diagram of the 3D-SIMM system (e) Lyapunov spectrum of the 3D-SIMM system (f) Bifurcation diagram of the 3D-SIMM system (g) Phase diagram of the CTBCS system (h) Lyapunov spectrum of the CTBCS system (i) Bifurcation diagram of the CTBCS system.

Setting the shifting constant is $b_1 = -3$. The chaotic behavior is present in the Fig. 1(g-i). Based on the Fig. 1(h), when the range of control parameter $r_1 \in [-20,20]$ with an increment of $\Delta r_1 = 0.01$. The chaotic system is enter chaos state. Especially, the system is hyper-chaotic when $r_1 \neq 1$.

B. THE RANDOMNESS OF NEW DISCRETE CHAOTIC SYSTEM

High randomness of the new discrete chaotic system relies strongly on complexity of two seed systems. In this section, the NIST SP 800-22 test package is introduced for measuring the randomness of chaotic sequences. This package has three indexes for scoring randomness. The first index is $P - value$. Set the confidence level is α, if the $P - value \geq 0.01$, it can prove that the sequence is randomness and pass the statistical test. For testing the $P - value$ of all sample block is subject to the uniform distribution. $P - value_T$ is introduced in this subsection. It is obtained based on the Eq. (5)

$$\chi^2 = \sum_{i=1}^{10} \frac{(F_i - 0.1s)^2}{0.1s} \tag{5}$$

where F_i is the number of $P - value$ in sub-interval i, and s is the sample size. Set the confidence level is α, if the $P - value_T \geq 0.0001$, then the sequences can be considered as randomness. That means the chaotic sequence has high-degree randomness. This is second index in the NIST test.

The third index is pass proportion of sample sequence. The result is based on the a serial date from the statistical test. Set the confidence level is α. The range of acceptable proportions is determined using the confidence interval defined as

$$\hat{P} = \sqrt{\frac{\hat{P} \cdot (1 - \hat{P})}{m}} \tag{6}$$

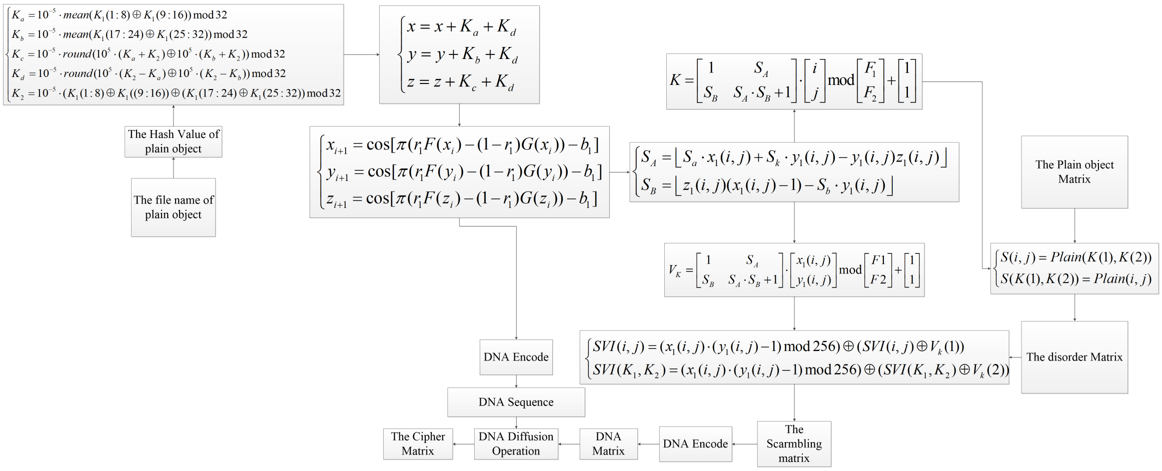

$K_a = 10^{-5} \cdot mean(K_1(1:8) \oplus K_1(9:16)) \bmod 32$
$K_b = 10^{-5} \cdot mean(K_1(17:24) \oplus K_1(25:32)) \bmod 32$
$K_c = 10^{-5} \cdot round(10^5 \cdot (K_a + K_2) \oplus 10^5 \cdot (K_b + K_2)) \bmod 32$
$K_d = 10^{-5} \cdot round(10^5 \cdot (K_2 - K_a) \oplus 10^5 \cdot (K_2 - K_b)) \bmod 32$
$K_2 = 10^{-5} \cdot (K_1(1:8) \oplus K_1((9:16)) \oplus (K_1(17:24) \oplus K_1(25:32)) \bmod 32$
The Hash Value of plain object
The file name of plain object
$x = x + K_a + K_d$
$y = y + K_b + K_d$
$z = z + K_c + K_d$
$x_{i+1} = \cos[\pi(r_1 F(x_i) - (1-r_1)G(x_i)) - b_1]$
$y_{i+1} = \cos[\pi(r_1 F(y_i) - (1-r_1)G(y_i)) - b_1]$
$z_{i+1} = \cos[\pi(r_1 F(z_i) - (1-r_1)G(z_i)) - b_1]$
$K = \begin{bmatrix} 1 & S_A \\ S_B & S_A \cdot S_B + 1 \end{bmatrix} \cdot \begin{bmatrix} i \\ j \end{bmatrix} \bmod \begin{bmatrix} F_1 \\ F_2 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
$S_A = \lfloor S_a \cdot x_1(i,j) + S_k \cdot y_1(i,j) - y_1(i,j) z_1(i,j) \rfloor$
$S_B = \lfloor z_1(i,j)(x_1(i,j) - 1) - S_b \cdot y_1(i,j) \rfloor$
The Plain object Matrix
$V_K = \begin{bmatrix} 1 & S_A \\ S_B & S_A \cdot S_B + 1 \end{bmatrix} \cdot \begin{bmatrix} x_1(i,j) \\ y_1(i,j) \end{bmatrix} \bmod \begin{bmatrix} F1 \\ F2 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
$S(i,j) = Plain(K(1), K(2))$
$S(K(1), K(2)) = Plain(i,j)$
DNA Encode
$SVI(i,j) = (x_1(i,j) \cdot (y_1(i,j) - 1) \bmod 256) \oplus (SVI(i,j) \oplus V_k(1))$
$SVI(K_1,K_2) = (x_1(i,j) \cdot (y_1(i,j) - 1) \bmod 256) \oplus (SVI(K_1,K_2) \oplus V_k(2))$
The disorder Matrix
DNA Sequence
The Cipher Matrix
DNA Diffusion Operation
DNA Matrix
DNA Encode
The Scarmbling matrix

FIGURE 2. The flow of encryption algorithm.

TABLE 1. The randomness test result of the new discrete system.

Test Name		Test sequence x		
		$P-value_{mean}$	$P-value_T$	Pass Rate
Frequency		0.4873	0.5544	1
Block Frequency		0.5031	0.5955	1
Runs		0.5176	0.2133	1
Longest Run		0.4849	0.3505	0.98
FFT		0.5011	0.3345	1
Universal		0.4915	0.3190	1
Approximate Entropy		0.5037	0.1223	1
Linear Complexity		0.5222	0.1373	0.99
Non Overlapping Template		0.5008	0.5144	0.9902
Overlapping Template		0.5341	0.5955	0.98
Cumulative Sums	Forward	0.4987	0.7981	0.99
	Reverse	0.4814	0.3191	0.99
Serial	$P-value_1$	0.4987	0.9835	0.99
	$P-value_2$	0.4814	0.4559	1
Random Excursions	$x=-4$	0.2687	0.2535	0.9833
	$x=-3$	0.2670	0.3781	0.9667
	$x=-2$	0.2784	0.2536	0.9667
	$x=-1$	0.2769	0.8881	0.9667
	$x=1$	0.2699	0.4373	0.9833
	$x=2$	0.3029	0.2757	0.9667
	$x=3$	0.2691	0.6718	0.9833
	$x=4$	0.3134	0.2133	1

where $\hat{P} = 1 - \alpha$, and m is the size of the test sample. The ideal pass proportion is 0.9960 when the $P - value \geq 0.01$. The testing result of seed system and new discrete chaotic system is present in Table (1-2).

III. THE ENCRYPTION SCHEME DESCRIPTION

The flow of algorithm is described clearly in this section. Firstly, the Arnold matrix is response for change the order and the value of plain 3D image. Secondly, the DNA encryption algorithm is adopted in the second round diffusion operation. Therefore, encrypted file has error space structure and cannot recognize. The whole encryption flow is shown in Fig 2.

A. THE PREPARATION OF ENCRYPTION ALGORITHM

This section is described the detail of preparation work. Firstly, the basic unit of 3D image is triangles. It is different from the pixel point with the 2D image. These triangles are constructed the shape of 3D image. Moreover, the triangle in the 3D image includes the coordinate of three directions. Therefore, the preparation work is to segment the 3D image by using these triangles. The segment algorithm is based on the Stereolithography. This algorithm can generate a number of triangles by 3D image. The example of segmentation is shown in Fig. (3).

TABLE 2. The randomness test result of the new discrete system.

		Test Sequence x		
Test Name		$P-value_{mean}$	$P-value_T$	Pass Rate
Random Excursions Variant	x=-9	0.2946	0.4373	1
	x=-8	0.2731	0.6025	1
	x=-7	0.2725	0.9114	1
	x=-6	0.2896	0.4373	1
	x=-5	0.2886	0.2992	1
	x=-4	0.2980	0.2328	1
	x=-3	0.2536	0.2709	0.9833
	x=-2	0.2627	0.7728	0.9333
	x=-1	0.2791	0.8623	0.95
	x=1	0.3228	0.8343	0.9833
	x=2	0.3081	0.8343	0.9833
	x=3	0.2791	0.3242	0.9833
	x=4	0.2916	0.9957	0.9833
	x=5	0.3169	0.9496	0.9833
	x=6	0.3119	0.9320	0.9833
	x=7	0.3264	0.4372	0.9833
	x=8	0.3304	0.2757	0.9833
	x=9	0.3125	0.4071	1

B. THE SECERT KEY GENERTOR

The secret key is determined by the system parameters and initial condition of discrete system. Firstly, for enhancing the security level of encryption algorithm, the SHA-256 hash function is adopted. The different plaintext file name can generate the different hash value. Based on the different hash value, the initial condition of discrete system is different. Therefore, the encryption algorithm can get different secret sequence.

1) Using the SHA-256 algorithm to generate the 256-bit secret key K of plain text 3D model file, the key will divide into 8-bit blocks k_i. Then, those bit blocks through XOR operation to obtain the new stream key

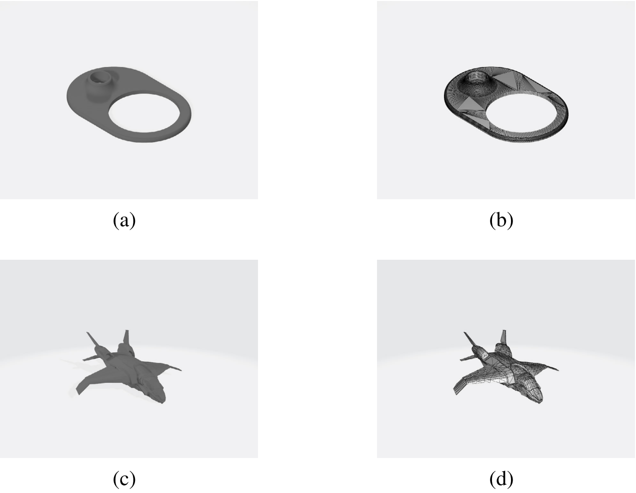

(a) (b) (c) (d)

FIGURE 3. **The example of segmentation with different 3D image:(a) the part of phonograph, (b) The distribution of segment triangle in the phonograph, (c) the Kun Jet (d) The distribution of segment triangle in the Kun Jet.**

as follows

$$K_i = K_{2i} \oplus K_{2i-1}. \tag{7}$$

where i is belong to [1,32]. Therefore, $K1$ has 32 group bit blocks. At least, the disturbance parameters are obtained according to the Eq. (8)

$$\begin{cases} K_a = 10^{-5} mean(K_1(1:8) \oplus K_1(9:16)) \bmod 32 \\ K_b = 10^{-5} mean(K_1(17:24) \oplus K_1(25:32)) \bmod 32 \\ K_2 = mean(round(10^5 \cdot (K_a + K_2) \oplus 10^5 \cdot (K_b + K_2))) \\ K_2 = 10^{-5} \cdot K_2 \bmod 32 \\ K_c = mean(round(10^5 \cdot (K_2 - K_a) \oplus 10^5 \cdot (K_2 - K_b))) \\ K_c = 10^{-5} \cdot K_c \bmod 32 \\ K_d = K_1(1:8) \oplus K_1(9:16) \oplus K_1(17:24) \\ \qquad \oplus K_1(25:32) \\ K_d = mean(K_d) \\ K_d = 10^{-5} \cdot K_d \bmod 32. \end{cases} \tag{8}$$

2) Inputting the initial condition of the discrete system as the secret key. The disturbance parameters have changed the value of the secret key. It will become the new initial condition of discrete chaotic system. The mathematical method of disturbance secret key is obtained as follows.

$$\begin{cases} x = x + K_a + K_d \\ y = y + K_b + K_d \\ z = z + K_c + K_d. \end{cases} \tag{9}$$

C. THE FLOAT NUMBER LEVEL ENCRYPTION BASED ON THE ARNOLD MATRIX SCRAMBLING-DIFFUSION SCHEME

1) Where the S_A and S_B are the parameter of Arnold matrix. The value of the parameter depended on the discrete chaotic sequence. The calculation principle of parameter matrix S are shown in Eq. (10)

$$\begin{cases} S_A = \lfloor S_a \cdot x_1(i,j) + S_k \cdot y_1(i,j) - y_1(i,j) \cdot z_1(i,j) \rfloor \\ S_B = \lfloor z1(i,j) \cdot (x1(i,j) - 1) - S_b \cdot y_1(i,j) \rfloor. \end{cases} \tag{10}$$

2) The Arnold matrix is used to generate the new coordinate of vertex for disorder the plain matrix. The scramble method of coordinates is shown in Eq. (11).

$$k = \begin{bmatrix} 1 & S_A \\ S_B & S_A \cdot S_B + 1 \end{bmatrix} \cdot \begin{bmatrix} i \\ j \end{bmatrix} mod \begin{bmatrix} F1 \\ F2 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{11}$$

where k is the new coordinates in scarmbling matrix.

3) In this step, the Arnold matrix is used to obtained the parameters of diffusion. The parameters are used to change the value of elements in new scarmbling matrix. The generated method of diffusion parameters are subject to Eq. (12) and Eq. (13)

$$V_k = \begin{bmatrix} 1 & S_A \\ S_B & S_A \cdot S_B + 1 \end{bmatrix} \cdot \begin{bmatrix} x_1(i,j) \\ y_1(i,j) \end{bmatrix} mod \begin{bmatrix} F1 \\ F2 \end{bmatrix}; \tag{12}$$

$$V_k = V_k + \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{13}$$

where V_k is the diffusion value.

4) Based on the result of V_k, the principle of diffusion is presented in Eq. (14)

$$\begin{cases} SVI(i,j) = (SVI(i,j) \oplus V_k(1)) \\ SVI(K_1, K_2) = (SVI(K_1, K_2) \oplus V_k(2)) \\ SVI(i,j) = SVI(i,j) \oplus (x_1(i,j) \cdot (y_1(i,j) - 1) \\ SVI(K_1, K_2) = SVI(K_1, K_2) \oplus (x_1(i,j) \cdot (y_1(i,j) - 1) \\ SVI(i,j) = SVI(i,j) \bmod 256 \\ SVI(K_1, K_2) = SVI(K_1, K_2) \bmod 256 \end{cases} \tag{14}$$

D. DNA LEVEL ENCRYPTION

The DNA level encryption is important step of algorithm. The purpose of this step is diffuse the value of coordinates matrix completely. At first, the DNA coding rules is described clearly in this section. Moreover, the flow of DNA encryotion is shown in this section.

1) DNA CODING RULES

This part is described the DNA coding rules and the calculation rules. According to the DNA encoding theory, each DNA sequence can present a piece of certain information in the image matrix. The DNA sequence is constructed by Adenine (A), Thymine (T), Cytosine (C), and Guanine (G). Therefore, the encoding rule based on the Watson-Crick complementary rule as shown in Table 3. Besides, the law of DNA calculation is shown in Table 4.

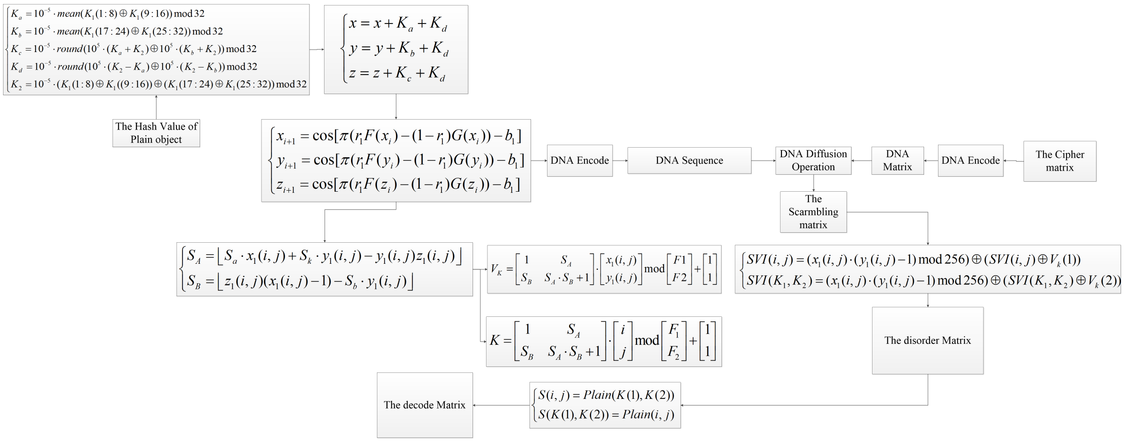


FIGURE 4. The flow of decryption algorithm.

TABLE 3. Table of DNA encode rule.

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

TABLE 4. Table of DNA addition and subtraction rule.

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

2) THE FLOW OF DNA LEVEL DIFFUSION

1) Setting the size of the DNA sequence is H × 4 × W. The 3D image matrix is transformed into this DNA sequence S1 by DNA encoding. The chaotic sequence is encoded by DNA encoding rule.
2) The disorder sequence D is obtained by scrambling operation. The scrambling operation is based on the principle of base complementary pairing. It is used to scrambling the combination of S1.
3) The sequence K1 is used to diffuse the matrix D. This operation can obtain the new cipher sequence C1.
4) The matrix C1 is decoded the double format. At the end, this matrix as the encryption result to generate the cipher image.

E. THE FLOW OF DECRYPTION ALGORITHM

The decryption algorithm can be considered as the inverse process compares with the encryption algorithm. The whole flow of the decryption algorithm is present in Fig 4.

1) Assuming the size of the encrypted file is $H \times W$. The decryption sequence is obtained from the Eq. (4). The initial condition and the disturbance parameter is fixed.
2) Set the size of recover space is $H \times W \times 4$. The data format of the cipher matrix is transformed DNA sequence. Also, the decryption sequence is encoded for reverse the DNA diffusion operation.
3) In this step, the algorithm will restore the DNA order of the cipher matrix. The decryption sequence is used to recover the original DNA code of the cipher matrix. The flow of rebuild is inverse processing compare with the DNA diffusio operation.
4) According to the Eq. (12-14), the value of vertex is recalculate by using the decryption sequence. The direction of recalculate is inverse compare with the diffusion operation. The decryption 3D solid model is obtained when this step is finished.
5) According to the Eq. (10-11), the vertex order of cipher matrix is recovered by using the decryption sequence. The flow of reorder the vertex point is inverse operation.

IV. THE SECURITY DEGREE ANALYSE

A. KEY SPACE ANALYSIS

In ideal condition, the size of secret key in encryption algorithm should be large than 2^{100} [10]. This size of key space can ensure ability of resist the brute force attack. On the basis of this encryption scheme, the construction of secret key should consist the initial condition and the parameters of chaotic system. Also, the SHA-256 hash value of the plain image is a important part in the secrte key. Therefore, the key space of proposed algorithm can approach 2^{754}. Table 5 presents the comparison result of key space. Obviously, the proposed algorithm has a larger key space compare with other algorithms.

TABLE 5. Table of key space.

The encryption scheme	Proposed algorithm	Ref. [38]	Ref. [39]	Ref. [29]	Ref. [8]	Ref. [28]
Key space	2^{754}	2^{465}	2^{256}	2^{224}	2^{599}	2^{240}

B. KEY SENSITIVE ANALYSIS

In the cryptosystem, highly sensitive of the secret key is very important feature for the encryption algorithm. A slight change cannot obtain the correct plaintext information.

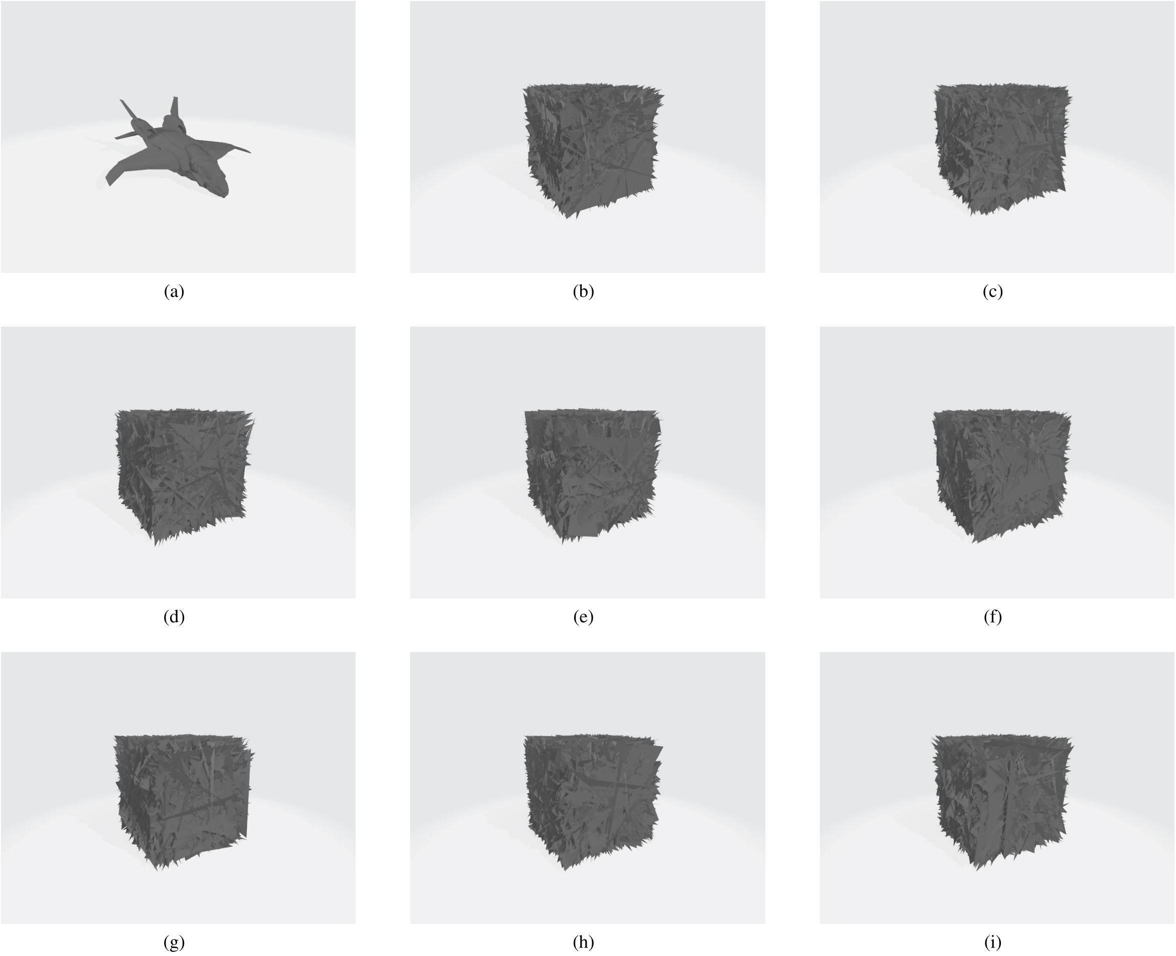

(a) (b) (c) (d) (e) (f) (g) (h) (i)

FIGURE 5. Sensitivity test result in decryption phase: (a) The correct decryption model (b)The initial condition $r + 10^{-15}$ (c)The initial condition $b + 10^{-15}$ (d)The initial condition $r_1 + 10^{-15}$ (e)The initial condition $b_1 + 10^{-15}$ (f)The initial condition $a + 10^{-15}$ (g)The initial condition $b_2 + 10^{-15}$ (h)The initial condition $c + 10^{-15}$ (i)The initial condition $r1 - 10^{-15}$.

TABLE 6. NPCR result in decryption phase (Initial condition:*r*,*b*,*r*1,*b*1).

Test condition	$r + 10^{-15}$	$r - 10^{-15}$	$b + 10^{-15}$	$b - 10^{-15}$	$r_1 + 10^{-15}$	$r_1 - 10^{-15}$	$b_1 + 10^{-15}$	$b_1 - 10^{-15}$
	0.9960	0.9960	0.9958	0.9964	0.9965	0.9961	0.9957	0.9961

TABLE 7. NPCR result in decryption phase (Initial condition:*a*,*b*2,*c*).

Test condition	$a + 10^{-15}$	$a - 10^{-15}$	$b_2 + 10^{-15}$	$b_2 - 10^{-15}$	$c + 10^{-15}$	$c - 10^{-15}$
	0.9958	0.9961	0.9961	0.9962	0.9961	0.9959

Where the initial condition of the discrete system is changed to test the key sensitive. The new parameters as a secret key to decrypt the cipher model file. Fig. (5) is shown that the simulation result. To measure the difference between the encryption model matrix and the error decryption model matrix, the NPCR method is adopted in the key sensitive analysis. When the initial condition of chaotic system is correct, the value of NPCR equal to zero. Set the $\Delta = \pm 10^{-15}$, Tables 6 and 7 are shown the different levels when the initial condition has little change.

C. THE ANTI-STATISTICAL ATTACK ABILITY ANALYSIS

In order to measure whether the algorithm can be resisted the statistical attack. In this part, the histogram of cipher vertex matrix and plaintext matrix are plotted. The analysis method is similar to the image encryption algorithm. In ideal conditions, the ideal cipher matrix can be considered as uniform distribution. Therefore, the chi-square test is used to prove whether this theory is correct. In this section, the transport plane model as the test sample. The result of histograms is present in Fig. (6). Moreover, the critical value is used to testing this assumption. The different critical value with 10%, 5%, and 1% probability are 284.3360, 293.2478 and 310.4574 respectively.

D. THE CORRELATIONAL ANALYSIS

In the plaintext matrix of the 3D image, the coordinate information of each column has strong correlation. Therefore, the statistical information of plaintext matrix needs to be hidden by reducing the correlation. This section is analyzed the correlational of cipher matrix and plaintext matrix. The associated equation of correlation as follow:

$$\gamma_{xy} = \frac{cov(x, y)}{\sqrt{D(X)D(Y)}}; \tag{15}$$

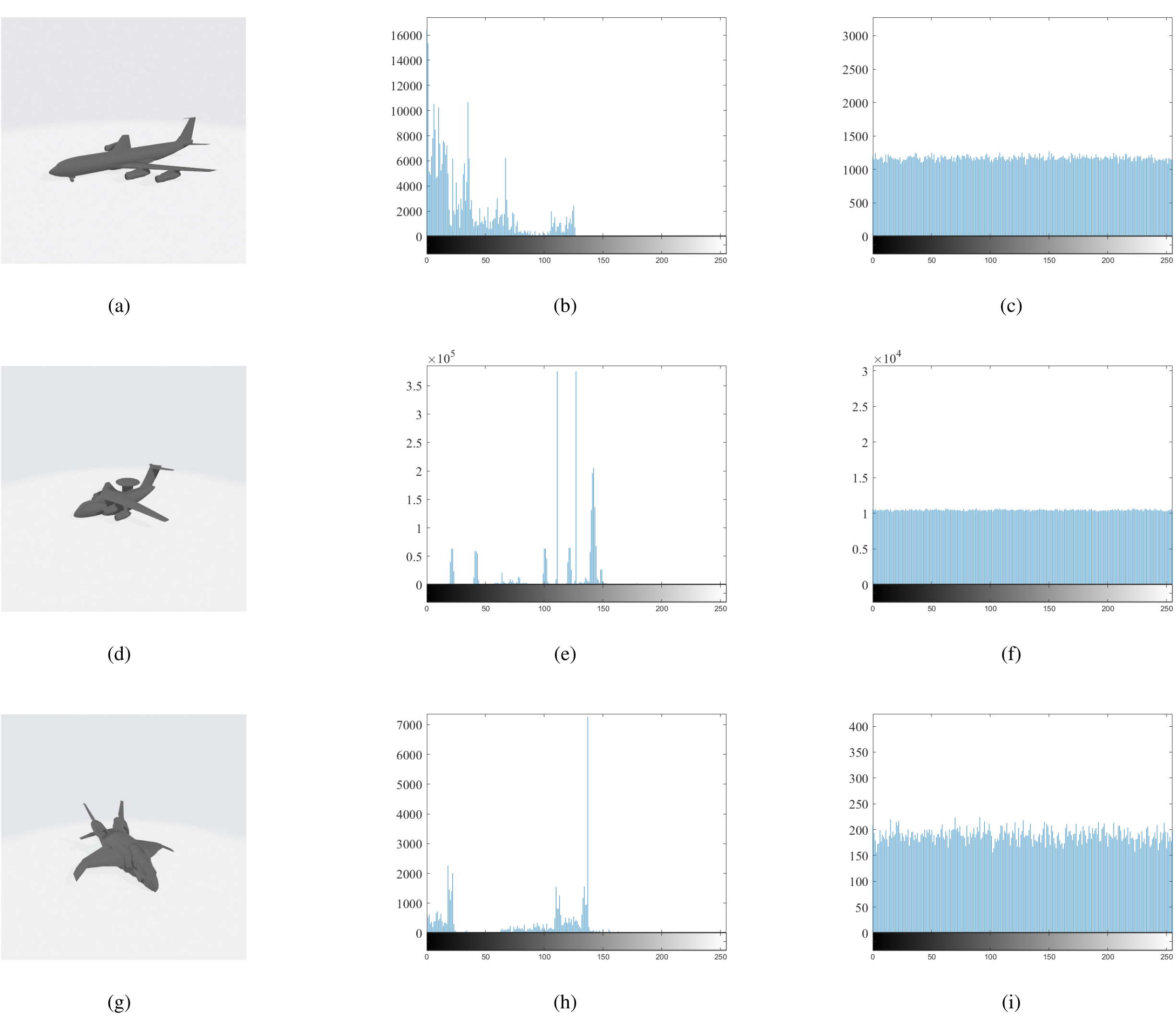
$$cov(x, y) = E(X - E(X)) - (Y - E(Y)); \tag{16}$$

TABLE 8. The table of χ^2 -value for different objects.

The model name	χ^2-value (plaintext)	χ^2 -value (Cipher)	Critical Value		
			$\chi^2_{0.1}$ (255)	$\chi^2_{0.05}$ (255)	$\chi^2_{0.01}$ (255)
Boeing-747	5629453.5524	226.8472	Pass	Pass	Pass
Air Early Warning Plane	473115.3675	247.4245	Pass	Pass	Pass
Kun Jet	408546.4986	245.4355	Pass	Pass	Pass

TABLE 9. The table of correlation coefficent with different directions.

The model name	Direction X		Direction Y		Direction Z	
	Plaintext	Cipher	Plaintext	Cipher	Plaintext	Cipher
Kun Jet	0.9763	0.9878	0.9869	0.0118	0.0062	3.792×10^{-4}
Air Early Warning	0.9982	0.9954	0.9975	-0.0041	0.0051	-0.0075
Boeing-747	0.9794	0.9992	0.9815	-0.0030	0.0002	-0.0004



(a) (b) (c)

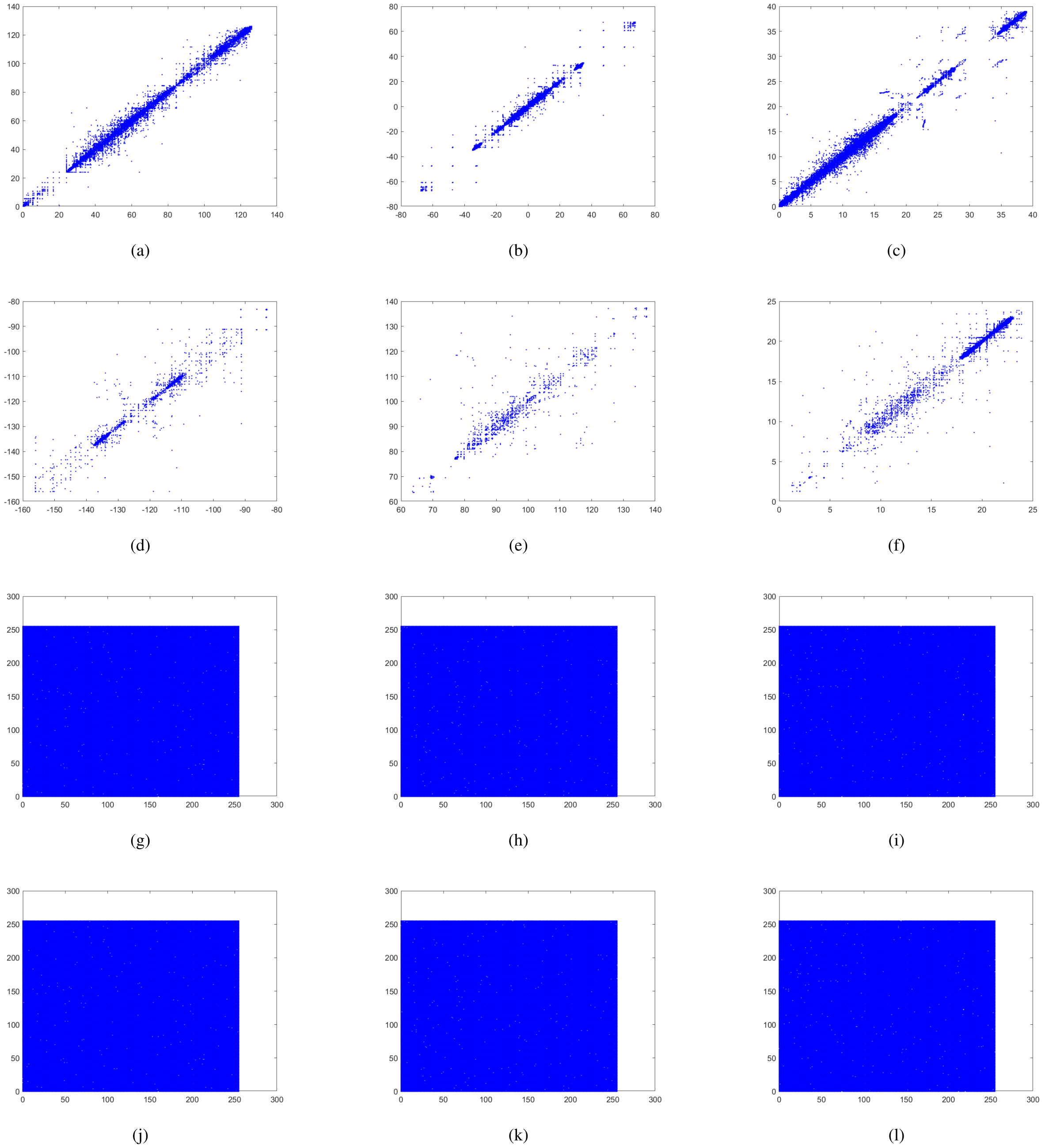
(d) (e) (f)

(g) (h) (i)

FIGURE 6. Sensitivity test result in decryption phase: (a) The correct decryption model (b)The initial condition $r + 10^{-15}$ (c)The initial condition $b + 10^{-15}$ (d)The initial condition $r_1 + 10^{-15}$ (e)The initial condition $b_1 + 10^{-15}$ (f)The initial condition $a + 10^{-15}$ (g)The initial condition $b_2 + 10^{-15}$ (h)The initial condition $c + 10^{-15}$ (i)The initial condition $r1 - 10^{-15}$.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i; \tag{17}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}[(x_i - E(x))]^2. \tag{18}$$



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

FIGURE 7. **The analyse result of coordinate distribution: The subfigures (a) to (f) are the plaintext image correlation distribution in x, y, and z directions. The subfigures (g) to (l) are the cipher image correlation distribution in x, y, and z directions.**

where, the expectation and variance of variable x are presented by $E(x)$ and $D(x)$ respectively. The $cov(x, y)$ is represent covariance of variable x. The correlation of one column between the plaintext vertex matrix and the encrypted matrix are illustrated in Fig 7.

E. THE ANTI-DIFFERENCE ATTACK ABILITY

NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are important security performance of encryption algorithm. Those analysis methods are used to testing the algorithm can resist the differential attack. Based on the characterizes of 3D image, the 3D image matrix is considering a special image matrix. Therefore, those analysis methods can adopt in the security analysis of 3D

TABLE 10. **NPCR result of the different 3D image.**

The model name	NPCR (mean)	Critical Value		
		$N^*_{0.05}$ (255) =99.5696%	$N^*_{0.01}$ (255) =99.5527%	$N^*_{0.001}$ (255) =99.5341%
Boeing-747	99.61%	Pass	Pass	Pass
Air Early Warning Plane	99.62%	Pass	Pass	Pass
Kun Jet	99.61%	Pass	Pass	Pass

TABLE 11. UACI result of the different 3D image.

The model name	UACI (mean)	Critical Value		
		$u^*_{0.05}+$ (255) =33.6447% $u^*_{0.05}-$ (255) =33.2824%	$u^*_{0.01}+$ (255) =33.7016% $u^*_{0.01}-$ (255) =33.2255%	$u^*_{0.001}+$ (255) =33.7677% $u^*_{0.001}-$ (255) =33.1594%
Boeing-747	33.44%	Pass	Pass	Pass
Air Early Warning Plane	33.43%	Pass	Pass	Pass
Kun Jet	33.42%	Pass	Pass	Pass

image encryption algorithm. The specific calculation method is shown as follows

$$\begin{cases} NPCR = \dfrac{\sum_{i,j} D(i,j)}{L} \times 100\% \\ UACI = \dfrac{1}{L}\sum_{i,j} \dfrac{|C(i,j) - C_1(i,j)|}{256} \times 100\%. \end{cases} \tag{19}$$

Setting the size of the 3D image is $H \times W$. The matrix C (i, j) is the cipher matrix. Then, the value of plain matrix is changed randomly. Therefore, the new cipher matrix C1 (i, j) is obtained. The symbolic function D (i, j) is determined by equation

$$D(i,j) = \begin{cases} 1 & C(i,j) \neq C_1(i,j) \\ 0 & C(i,j) = C_1(i,j). \end{cases} \tag{20}$$

The strictly critical score of NPCR and UACI were adopted in this section. These index are used to measuring the result of NPCR and UACI are avaliable [40]. Setting the number of coordinates in a plaintext matrix is G. Besides, the value of bitxor in diffusion operation is L. The critical score of NPCR is obtained as follows:

$$N^*_a = \frac{G - \Phi^{-1}(a)\sqrt{\frac{G}{L}}}{G+1}. \tag{21}$$

The ideal condition is the NPCR value is greater than N^a_*. It means this result is avaliable. The critical value of UACI with given as follow

$$\begin{cases} u^{*-}_a = \mu_u - \Phi^{-1}(\frac{\alpha}{2})\sigma_u \\ u^{*+}_a = \mu_u + \Phi^{-1}(\frac{\alpha}{2})\sigma_u, \end{cases} \tag{22}$$

where

$$\sigma_u = \frac{G+2}{3G+4}, \tag{23}$$

and

$$\sigma_u = \frac{(G+2)(G^2+2G+3)}{18(G+1)^2 GL}. \tag{24}$$

The ideal condition of UACI is the result of UACI with the range (u^{-a}_*, u^{+a}_*). It can prove that the result of UACI with the acceptable range. Therefore, this encryption algorithm has enough ability to resist the diffenece attack. The simulation results are shown in Tables 11 and 12. The results are close to the ideal value. It can demonstrate that this algorithm has good performance when the cipher is suffered the different-attack.

V. CONCLUSION

This paper designed a novel encryption algorithm for 3D image file based on the new discrete chaotic system. Firstly, the chaotic characterize analysis show that this chaotic system has good characteristics such as more complex dynamical behavior. Therefore, this chaotic system is suitable to apply to encode the 3D image file. This measure can add the difficult of malicious access. Secondly, this encryption algorithm is changed the scrambling-diffusion concept. In the scarmbling operation, the value of plaintext matrix is changed. It can disorder the spatial distribution more effectively. The hash function can generated different initial conditions based on the different filename. It is can enhance the security level. Finally, the performance indexes of algorithm security show that this algorithm has ability to resist different kinds of attacks. In conclusion, this algorithm has good encryption characteristics and protects the 3D image files information more effectively. This encryption scheme can embed the 3D model design software. Before file transfer, this algorithm can encode the information of the 3D image files and prevent the attacker to decode it. Moreover, this encryption scheme provided another realization way for 3D image file security.

REFERENCES

[1] F. P. Melchels, J. Feijen, and D. W. Grijpma, "A review on stereolithography and its applications in biomedical engineering," *Biomaterials*, vol. 31, no. 24, pp. 6121–6130, 2010. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/20478613

[2] C. L. Ventola, "Medical applications for 3D printing: Current and projected uses," *Pharmacy Therapeutics*, vol. 39, no. 10, p. 704, 2014.

[3] A. Ambrosi and M. Pumera, "3D-printing technologies for electrochemical applications," *Chem. Soc. Rev.*, vol. 45, no. 10, pp. 2740–2755, 2016.

[4] W. Kaminsky, T. Snyder, J. Stone-Sundberg, and P. Moeck, "One-click preparation of 3D print files (* *.Stl, *.Wrl) from *.Cif (crystallographic information framework) data using Cif2 VRML," *Powder Diffraction*, vol. 29, no. S2, pp. S42–S47, Dec. 2014.

[5] A. C. Brown and D. de Beer, "Development of a stereolithography (STL) slicing and G-code generation algorithm for an entry level 3-D printer," in *Proc. Africon*, Sep. 2013, pp. 1–5.

[6] M. Éluard, Y. Maetz, and G. Doërr, "Geometry-preserving encryption for 3D meshes," *Actes de COmpression et REprsentation des Signaux Audiovisuels*, pp. 7–12, 2013, doi: 10.13140/RG.2.1.3925.6165.

[7] B. Raj, L. Jani Anbarasi, M. Narendra, and V. J. Subashini, "A new transformation of 3D models using chaotic encryption based on arnold cat map," in *Proc. Int. Conf. Emerg. Internetw., Data Web Technol.*, vol. 29, 2019, pp. 322–332.

[8] X. Jin, S. Zhu, C. Xiao, H. Sun, X. Li, G. Zhao, and S. Ge, "3D textured model encryption via 3D lu chaotic mapping," *Sci. China Inf. Sci.*, vol. 60, no. 12, Dec. 2017, Art. no. 122107.

[9] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[10] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[11] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and dna computing," *Int. J. Modern Phys. C*, vol. 28, no. 5, Art. no. 1750069, 2017.

[12] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 8, no. 8, pp. 29–41, 1989.

[13] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[14] G. Millerioux, J. M. Amigo, and J. Daafouz, "A connection between chaotic and conventional cryptography," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 6, pp. 1695–1703, Jul. 2008.

[15] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

[16] W. Liu, K. Sun, and S. He, "SF-SIMM high-dimensional hyperchaotic map and its performance analysis," *Nonlinear Dyn.*, vol. 89, no. 4, pp. 2521–2532, Sep. 2017.

[17] C.-L. Li, Z.-Y. Li, W. Feng, Y.-N. Tong, J.-R. Du, and D.-Q. Wei, "Dynamical behavior and image encryption application of a memristor-based circuit system," *AEU Int. J. Electron. Commun.*, vol. 110, Oct. 2019, Art. no. 152861.

[18] Aqeel-ur-Rehman, X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," *Optik Int. J. Light Electron Opt.*, vol. 153, pp. 117–134, Jan. 2018.

[19] P. Li, J. Xu, J. Mou, and F. Yang, "Fractional-order 4D hyperchaotic memristive system and application in color image encryption," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, p. 22, Dec. 2019.

[20] L.-M. Zhang, K.-H. Sun, W.-H. Liu, and S.-B. He, "A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations," *Chin. Phys. B*, vol. 26, no. 10, Sep. 2017, Art. no. 100504.

[21] W. Liu, K. Sun, Y. He, and M. Yu, "Color image encryption using three-dimensional sine ICMIC modulation map and DNA sequence operations," *Int. J. Bifurcation Chaos*, vol. 27, no. 11, Oct. 2017, Art. no. 1750171.

[22] J. Mou, F. Yang, R. Chu, and Y. Cao, "Image compression and encryption algorithm based on hyper-chaotic map," *Mobile Netw. Appl.*, 2019, doi: 10.1007/s11036-019-01293-9.

[23] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019.

[24] F. Yang, J. Mou, K. Sun, Y. Cao, and J. Jin, "Color image compression-encryption algorithm based on fractional-order memristor chaotic circuit," *IEEE Access*, vol. 7, pp. 58751–58763, 2019.

[25] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.

[26] L. Gong, C. Deng, S. Pan, and N. Zhou, "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," *Opt. Laser Technol.*, vol. 103, pp. 48–58, Jul. 2018.

[27] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "A 3D object encryption scheme which maintains dimensional and spatial stability," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 409–422, Feb. 2015.

[28] X. Wang, M. Xu, and Y. Li, "Fast encryption scheme for 3D models based on chaos system," *Multimedia Tools Appl.*, vol. 78, no. 23, pp. 33865–33884, Dec. 2019.

[29] X. Jin, Z. Wu, C. Song, C. Zhang, and X. Li, "3D point cloud encryption through chaotic mapping," in *Advances in Multimedia Information Processing—PCM* (Lecture Notes in Computer Science), vol. 9916, E. Chen, Y. Gong, and Y. Tie, Eds. Cham, Switzerland: Springer, 2016, doi: 10.1007/978-3-319-48890-5_12.

[30] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

[31] M. E. Goggin, B. Sundaram, and P. W. Milonni, "Quantum logistic map," *Phys. Rev. A, Gen. Phys.*, vol. 41, no. 10, pp. 5705–5708, May 1990. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/9902961

[32] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, Dec. 2012.

[33] A. Akhshani, A. Akhavan, A. Mobaraki, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 1, pp. 101–111, Jan. 2014.

[34] C. Jin and H. Liu, "A color image encryption scheme based on arnold scrambling and quantum chaotic," *IJ Netw. Secur.*, vol. 19, no. 3, pp. 347–357, 2017.

[35] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, pp. 92–102, Aug. 2019.

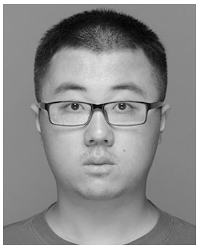
[36] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Process.*, vol. 93, no. 11, pp. 2986–3000, Nov. 2013.

[37] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 511–529, Jul. 2015.

[38] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Process.*, vol. 168, Mar. 2020, Art. no. 107340.

[39] A. M. ı. del Rey, "A method to encrypt 3D solid objects based on three-dimensional cellular automata," in *Proc. Int. Conf. Hybrid Artif. Intell. Syst.* Cham, Switzerland: Springer, 2015, pp. 427–438.

[40] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun. (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.



JI XU received the B.E. degree from the Shengli College, China University of Petroleum, China, in 2017. He is currently pursuing the Ph.D. degree with Dalian Polytechnic University, Dalian, China. His main research interests include chaos theory and chaotic digital image cryptosystems.

CHEN ZHAO received the B.S. degree in food science and engineering from Dalian Polytechnic University, Dalian, China, and the M.S. degree in economics from the Dongbei University of Finance and Economics, Dalian. She is currently a Professor with the School of Engineering Practice and Innovation-Entrepreneurship Education, Dalian Polytechnic University. Her current research interests include marketing management, entrepreneurship management, and higher education management.

JUN MOU received the B.S., M.S., and Ph.D. degrees in physics and electronics from Central South University, Changsha, China. He is currently an Associate Professor with the School of Information Science and Engineering, Dalian Polytechnic University, China. His main research interests include nonlinear system control, secure communication, power system automation, and smart grid research.