Dynamic analysis of New Two Dimensional Fractional-order Discrete Chaotic Map and Its application in Cryptosystem

Ze-Yu Liu

College of Science
Northwest A&F University, Yangling District, 712100, Shaanxi P. R. China.

Tie-Cheng Xia

College of Science
Shanghai University, Shanghai, 200444, Shanghai, P. R. China

Ye Hu

Department of mathematics
Lvliang University, Lvliang , 033000, Shanxi, P. R. China

Abstract

A new fractional difference equation 2D-TFCDM based on Caputo derivative is proposed. Using the bifurcation diagram, the maximum Lyapunov exponent and the phase diagram, the numerical solutions of the fractional difference equations are obtained, and the chaotic behavior is observed numerically. After encrypting the key with elliptic curve cryptosystem, the fractional map is developed as an encryption algorithm and applied to color image encryption. Finally, the proposed encryption system is systematically analyzed from five main aspects, and the results show that the proposed encryption system has a good encryption effect.

Keywords: Bifurcation, Caputo fractional derivative, Fractional discrete map, Cryptology design, Elliptic Curve Cryptosystem

2010 MSC: 26A33, 34F10, 39A10

☆Corresponding author email: liuzeyu_90@163.com

1. Introduction

Chaos is a complex dynamical behavior produced by nonlinear systems, which can produce pseudo-random chaotic sequences, and a chaotic encryption method is proposed based on this property of chaotic systems. Chaos encryption is a popular encryption method today, thanks to the randomness and sensitivity of chaotic encryption.The main principle of chaotic encryption is to use the pseudo-random chaotic sequence generated by the chaotic system, as the encryption sequence of information encryption.Whether enough chaotic pseudo-random sequence is the key to whether chaotic encryption is difficult to reconstruct, analyze and predict. So far, multiple algorithms have been implemented for chaos-based information encryption.

During the past decades, the discrete dynamic behaviors of fractional difference equations and its applications in information security has been paid a lot of attention[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]. Numerous results have been gotten for discrete fractional calculus. Fractional discrete Rossler system studied by Azil [11], Khennaoui studied the attractor of three-dimensional fractional Henon mapping [14], and Ouannas studied the dynamics, control and synchronization of fractional Ikeda system and the discrete fractional duffing system [12, 13] and discrete fractional order Duffing systems. He studied the chaotic dynamic behavior of fractional discrete time SIR epidemic model with inoculation [16]. Zhu constructs an image encryption scheme using a newly designed two-dimensional discrete fractional chaotic map[17]. Shi studied the chaotic dynamical behavior of fractional order delay financial systems[24]. Ma modified the complex networks into fractional order one and observe its dynamic behaviours[18]. Chen studied the fractional order discrete improved Henon map [19] and applied it into image encryption. Xu studied the fractional-order chaos system of Hopfield neural network [20].

Compared with the fruitful achievements of continuous fractional calculus, there are few researches on fractional difference equations and its applications. More recently, Wu and Baleanu contributed to the theoretical development of

Caputo fractional difference equations and their application.

Menezes-vanstone Elliptic Curve cryptosystem (MVECC) is fast and effective algorithm to encrypt keys, and it achieve the same level of security with smaller key sizes and higher computational efficiency [37].

Fiaz studied the generalization of synchronization of three-dimensional fractional chaotic systems [22]. Barba-franco studied the dynamical behavior of a system consisting of three fractional Duffing oscillators coupled together[23]. Image encryption with fractional calculus is booming nowadays, such as fractional-order one dimensional logistic map [25], fractional-order laser high dimensional system [27] and fractional one dimensional chaotic map [31]. All of the system mentioned above took use of continuous fractional calculus.

In [33], discrete fractional calculus is proposed for image encryption utilizing fractional chaotic time series. Afterwards, many information security methods are proposed within fractional difference equation[28, 29, 31, 30, 32]. However, there are few 2-dimensional chaotic map based on fractional-order difference at present.

On this basis, our main purpose is to introduce a new fractional map with its chaotic behavior detected. Then, new cryptosystem is proposed with key generated by MVECC. The content of this paper is arranged as follows: In the second part, we review the definition and properties of discrete fractional difference. Then, in the third part, we give the introduction of MVECC. In Section IV, we formulate the fractional 2D-TFCDM and observe the bifurcation with diagrams, maximal Lyapunov exponent (MLE) diagrams and phase diagrams with varying orders, coefficients and initial values. Section V introduces the application of information security in image encryption. In the sixth part, the image encryption results of the fifth part are analyzed. Finally, some conclusions are given.

2. Propaedeutic knowledge

In this section, we will introduce the definition of fractional difference. In discrete fractional difference, $f(n)$ is the discrete form of $f(i)$. $\mathbb{N}_b = \{b, b+1, b+2, \ldots\}$ ($b \in \mathbb{R}$ fixed) said the isolation time scale. $\Delta f(i) = f(i+1) - f(i)$ is the difference operator defined by

Definition 2.1 **[3]** Assuming $\alpha > 0$ and $w : \mathbb{N}_b \to \mathbb{R}$. Let the fractional sum of order α be

$$\Delta_b^{-\gamma} w(i) := \frac{1}{\Gamma(\gamma)} \sum_{s=b}^{i-\gamma} (i - \delta(s))^{(\gamma-1)} w(s), i \in \mathbb{N}_{b+\gamma}, \tag{1}$$

where b is the starting point, $\delta(s) = s+1$ and $i^{(\gamma)}$ is the falling function defined as

$$i^{(\gamma)} = \frac{\Gamma(i+1)}{\Gamma(i+1-\gamma)}. \tag{2}$$

The Gamma function is denoted by $\Gamma(\cdot)$ and is defined as

$$\Gamma(i) = \int_0^{+\infty} e^{-x} x^{i-1} dx, i > 0. \tag{3}$$

Definition 2.2 **[4]** Let Caputo fractional difference with α order be defined as

$$\begin{aligned} {}^C\Delta_b^{\gamma} w(i) :&= \Delta_b^{-(m-\gamma)} \Delta^m w(i) \\ &= \frac{1}{\Gamma(m-\gamma)} \sum_{s=b}^{i-(m-\gamma)} (i - \delta(s))^{(m-\gamma-1)} w(s), \\ & i \in \mathbb{N}_{b+m-\gamma}, m = [\gamma] + 1, \end{aligned} \tag{4}$$

where $1 > \alpha > 0$, $\alpha \notin \mathbb{N}$ and $w(i) \in \mathbb{N}_{b_0}$.

Theorem 2.1 **[5]**the equivalent discrete integral formula of (5)

$$\begin{aligned} &{}^C\Delta_b^{\gamma} w(i) = f(i+\gamma-1, w(i+\gamma-1)), \\ &\Delta^k w(b) = w_k, m = [\gamma] + 1, k = 0, \ldots, m-1 \end{aligned} \tag{5}$$

can be obtained as

$$\begin{aligned} w(n) =& w_0(i) + \frac{1}{\Gamma(\gamma)} \sum_{s=b+m-\gamma}^{i-\gamma} (i - \delta(s))^{(\gamma-1)} \\ & \times f(s+\gamma-1, w(s+\gamma-1)), i \in \mathbb{N}_{b+m}, \end{aligned} \tag{6}$$

the starting value in (6) reads

$$w_0(i) = \sum_{j=0}^{m-1} \frac{(i-b)^{(j)}}{j!} \Delta^j w(b). \tag{7}$$

From formula (4) to (6), $w(i)$ is a preserve function in the isolated definition on time scale $\mathbb{N}_b$ while a domain change from $\mathbb{N}_{b+m-\gamma}$ to $\mathbb{N}_{b+m}$.

3. Elliptic Curve Cryptosystem (ECC)

3.1 Definition of Elliptic Curve(EC) An EC E defined over the prime field F_p is the set of (x, y) satisfying the equation:

$$E : y^2 \equiv x^3 + dx + f(\mod p). \tag{8}$$

More precisely, it is the set of such solutions together with a infinity point O, where $d, f \in F_p, p \neq 2, 3$ and fit with the condition $4d^3 + 27f^2 \neq 0$. [38].

3.2 EC Operations

Let $R = (a_1, b_1)$, then $-R = S = (a_1, -b_1)$ is defined with $R + S = O$[38].

If points $R = (a_1, b_1)$ and $S = (a_2, b_2)$ lie on an EC E defined by Equation (8), then $R + S = T$ is computed in (9) and also lies on E[38]:

$$R + S = \begin{cases} T = (a_3, b_3), R \neq -T, \\ O, a_1 = a_2(\mod p), b_1 + b_2 = 0(\mod p). \end{cases} \tag{9}$$

where

$$\begin{aligned} a_3 &\equiv (\xi^2 - 2a_1)(\mod p), \\ b_3 &\equiv (\xi(a_1 - a_3) - b_1)(\mod p). \end{aligned} \tag{10}$$

and

$$\xi = \begin{cases} \frac{(b_2 - b_1)}{(a_2 - a_1)}, P \neq Q, \\ \frac{3a_1^2 + d}{2b_1}, P = Q. \end{cases} \tag{11}$$

The scalar multiplication can be defined by

$$kR = \underbrace{R + R + \cdots + R}_{k-times}, \tag{12}$$

where $k \in \mathbb{Z}$.

Definition 3.3 The order of EC is denoted by $\#E$ and is defined as the number of points on the curve.[38]

Definition 3.4 $ord(P)$ refer to the smallest $n \in \mathbb{Z}^+$ such that $nP = O$.

Definition 3.5 $P \in E(F_p)$ is called a generation point if $ord(P) = \#E$.

Definition 3.6: MVECC

MVECC is a public key cryptosystem with two users Arnold and Blain[37].

When Arnold want to send a message $M = (m_1, m_2) \in \mathrm{Z}_p^* \times \mathrm{Z}_p^*$ to Blain, they do the setups as follows:

1.Arnold makes an agreement with Blain about the base point β and the EC $E(F_p)$.

2.Blain chooses a private key S_B with nobody knows and computes $P_B = S_B \cdot \beta$ $(0 \leqq S_B < ord(\beta))$ as his public key.

3.Arnold first chooses the private key S_A randomly $(0 \leqq S_A < ord(\beta))$, and computes his public key $P_A = S_A \cdot \beta$. Secondly, Arnold computes $(s_1 \cdot s_2)$ as the secret key by formula (13)

$$(s_1 \cdot s_2) = S_A \cdot P_B = S_A \cdot S_B \cdot \beta \tag{13}$$

Then Arnold calculate the ciphered message by

$$\begin{aligned} c_1 &= m_1 * s_1 \mod p \\ c_2 &= m_2 * s_2 \mod p \end{aligned} \tag{14}$$

4.The ciphertext $\{P_A, (c_1, c_2)\}$ is sent to Blain. Blain firstly get the secret key by $(s_1, s_2) = S_B \cdot P_A$, then he computes (15)

$$\begin{aligned} m_1 &= c_1 * s_1^{-1} \mod p \\ m_2 &= c_2 * s_2^{-1} \mod p \end{aligned} \tag{15}$$

to get the plaintext $M = (m_1, m_2)$[37].

Any adversary who only knows the public key P_A and P_B but don't know the private keys S_A and S_B is very difficult to get the message M. Moreover, if $\#E$ is a prime number, it will be more difficult to break up the cryptosystem[38]. Therefore, MVECC is an efficient and secure technique for secret message encryption.

4. Fractional 2D-TFCDM and its Dynamical Characteristics

In the recent paper [39], the first 2D-TFCDM is introduced below,

$$\begin{cases} u_{n+1} = l_1 sin(w_n), l_1 = 10, \\ w_{n+1} = l_2 u_n sin(w_n) - l_3 u_n cos(w_n), l_2 = 1.7, l_3 = 0.556. \end{cases} \tag{16}$$

Consider the Caputo-like delta difference equation modified by the 1st 2D-TFCDM:

$$\begin{cases} {}^C\Delta_b^\gamma u(i) = l_1 sin(w(i+\gamma-1)) - u(i+\gamma-1), 0 < \gamma < 1, i \in N_{b+1-\gamma}, \\ w(n) = l_2 u(n-1) sin(w(n-1)) - l_3 u(n-1) cos(w(n-1)), l_2 = 1.7, l_3 = 0.556. \end{cases} \tag{17}$$

According to Theorem 2.1, with $0 < \gamma < 1$, the equivalent discrete numerical formula for 1 is as follows,

$$\begin{cases} u(n) = u(0) + \frac{1}{\Gamma(\gamma)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\gamma)}{\Gamma(n-j+1)} [l_1 sin(w(j-1)) - u(j-1)], \\ w(n) = l_2 u(n-1) sin(w(n-1)) - l_3 u(n-1) cos(w(n-1)), l_2 = 1.7, l_3 = 0.556. \end{cases} \tag{18}$$

Compared with integer-order maps, the dynamical behaviors of Caputo fractional chaotic map is more complex, and the value of $u(n)$ is strongly dependent on that of $u(0), ..., u(n-1)$. By utilizing (16), we draw the bifurcation graphs 1 and 5 with the step size 0.005. Similarly, by (18), we draw the bifurcation graphs 2 and 6. Through the analysis of the bifurcation graph, we can obtain the interval where chaos occurs, that is, in this region, the sequence generated by the numerical formula is well chaotic. When we change the value of the

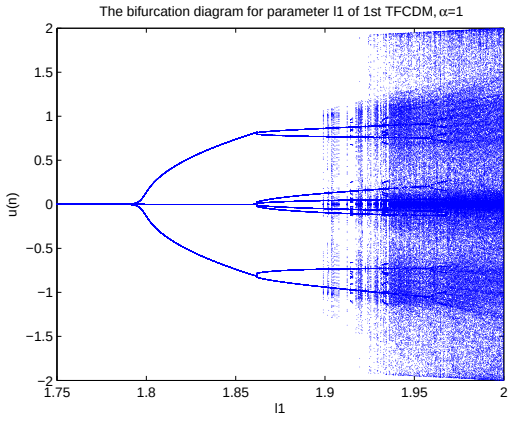


Figure 1: Bifurcation graph for the 1st 2D-TFCDM map with l_1 versus $u(n)$.

difference order, the chaotic zone also changes somewhat. The variation in the bifurcation graph 1,2,5 and 6 illustrates and explains this. In this way, we can generate a chaotic sequence for image encryption.

Set $\gamma = 1, u(0) = 0.19, W(0) = 0.06, N = 200$, the bifurcation graph is plotted in Figure 1 with the step size equal to 0.01. Figure 2 is an similar bifurcation graph with the different order $\gamma = 0.8$. As the figure shows, the chaotic region depends on the varying order γ clearly.

In Figure 3, for $\gamma = 1$, we use the Jacobian algorithm to obtain the MLE. The MLE is positive somewhere, which is corresponding to the chaotic region in Figure 1.

Similarly, another fractional difference equation is obtained:

$$\begin{cases} {}^{C}\Delta_{\beta}^{a} w(i) & = l_2 u(i+\gamma-1) sin(w(i+\gamma-1)) - l_3 u(i+\gamma-1) cos(w(i+\gamma-1)) \\ & \quad -w(i+\gamma-1), 0 < \gamma < 1, i \in N_{b+1-\gamma}, \\ u(n) & = l_1 sin(w(n-1)), l_1 = 10, l_3 = 0.556. \end{cases} \tag{19}$$

And the following fractional discrete numerical formula for parameters l_3 is also got:

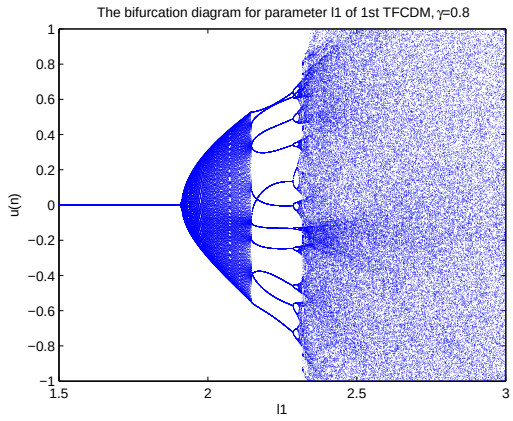


Figure 2: Bifurcation graph for the 1st 2D-TFCDM map with l_1 versus $u(n)$, γ=0.8.

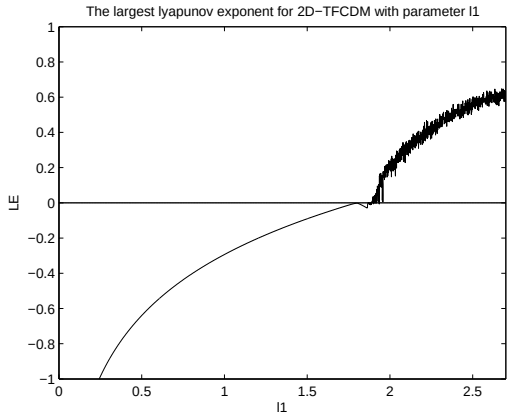


Figure 3: MLE for the 1st 2D-TFCDM map with l_1.

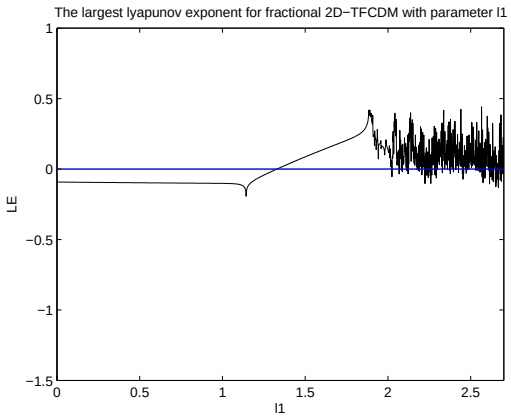


Figure 4: MLE for the 1st 2D-TFCDM map with l_1, γ=0.8.

$$\begin{cases} w(n) & = w(0) + \frac{1}{\Gamma(\gamma)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\gamma)}{\Gamma(n-j+1)} [l_2 u(j-1) sin(w(j-1)) - l_3 u(j-1) cos(w(j-1)) \\ & \quad -w(j-1)], l_1 = 10, l_3 = 0.556, \\ u(n) & = l_1 sin(w(n-1)). \end{cases} \tag{20}$$

We can also get the bifurcation graph, the MLE for formula (20).

With 301 different initial values set, we draw the phase portrait of formula (16).Then we consider the cases of fractional difference γ=0.9 and γ=0.8 in figure 10,11 respectively.

5. Applications

Now we apply the fractionalized map in information security fields. Consider (18) as an algorithm, $u_0, w_0, \gamma, l_1, l_2, l_3$ are set as keys for encryption. The encryption algorithm is designed into 3 parts in this paper.

5.1. Keys delivery with MVECC

Suppose that we have E be an EC define over F_{100357} with $d = 1, f = 6$ and $p = 100357$ in (8). After calculation, $\#E = 100169$ and it is a prime number, therefore E is a safe EC.

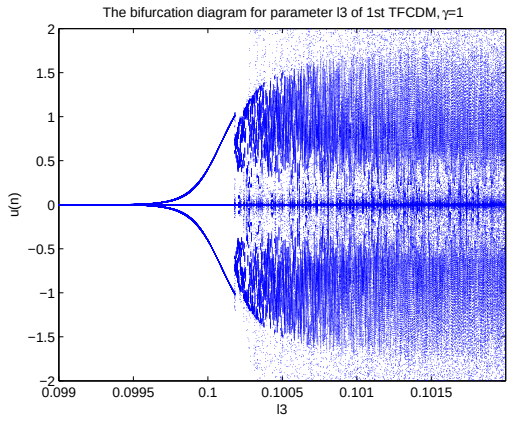


Figure 5: Bifurcation graph for the 1st 2D-TFCDM map with l_3 versus $u(n)$.

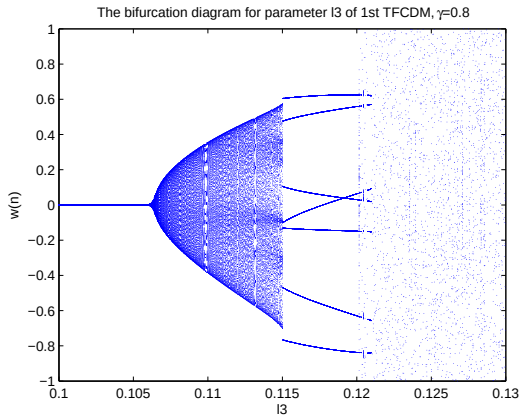


Figure 6: Bifurcation graph for the 1st 2D-TFCDM map with l_3 versus $u(n)$, γ=0.8.

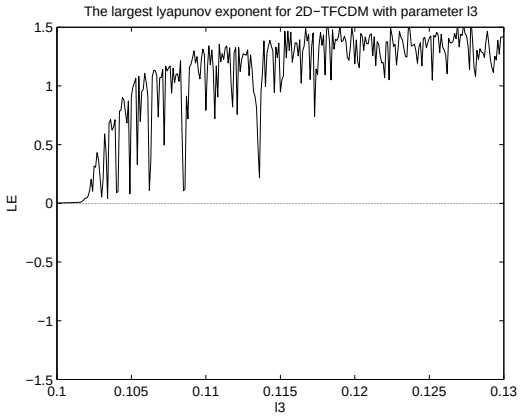


Figure 7: MLE for the 1st 2D-TFCDM map with l_3.

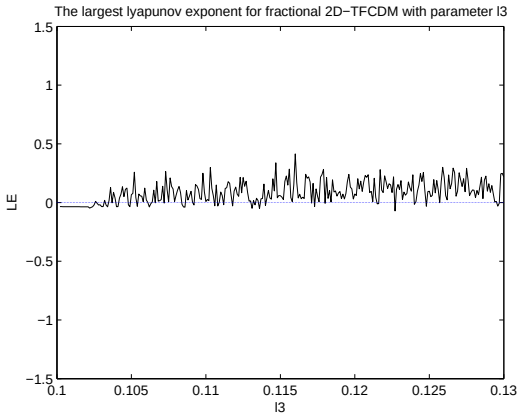


Figure 8: MLE for the 1st 2D-TFCDM map with l_3, γ=0.8.

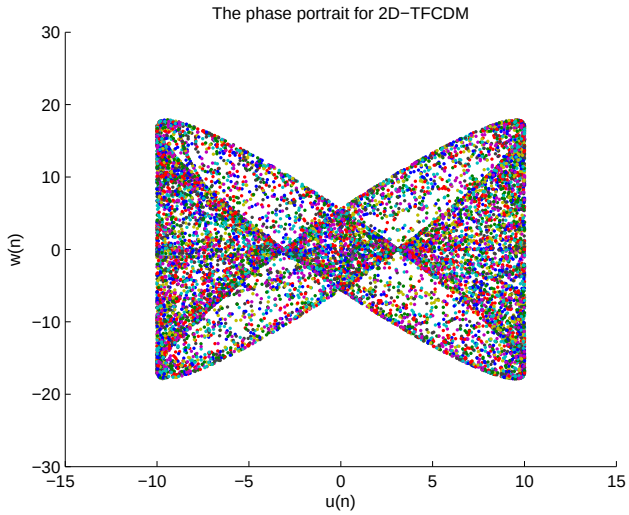


Figure 9: The phase space of the 1st TFCDM map for $l_1 = 6, l_2 = 0.3, l_3 = 0.6$ and γ=1.

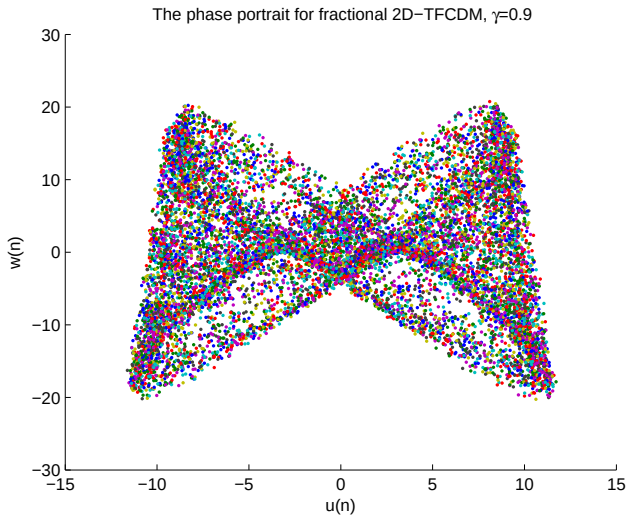


Figure 10: The phase space of the 1st TFCDM map for $l_1 = 6, l_2 = 0.3, l_3 = 0.6$ and γ=0.9.

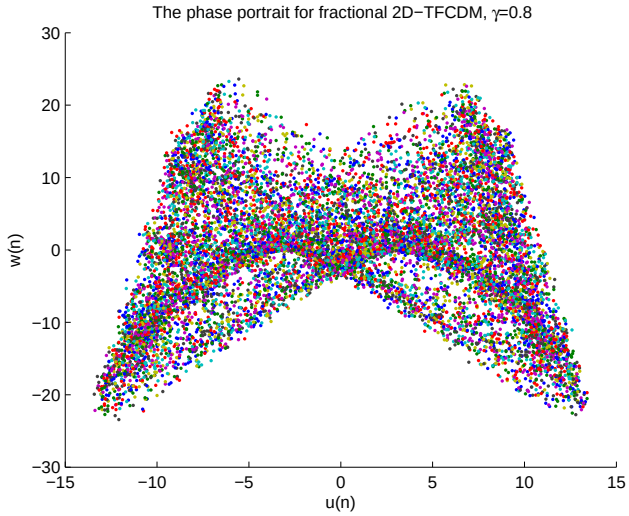


Figure 11: The phase space of the 1st TFCDM map for $l_1 = 6, l_2 = 0.3, l_3 = 0.6$ and γ=0.8.

Set $M = (m_1, m_2) = (7123, 45600)$, namely, $\gamma = 0.7123456$, $\beta = (2, 4)$. Arnold keep the secret key $S_A = 9768$, then he calculate his public key $P_A = S_A\beta = (43113, 45139)$. Blain Select $S_B = 1024$, then he get $P_B = S_B\beta = (8482, 90068)$. Before the key delivery, $(s_1, s_2) = S_BP_A = (16723, 84616) = S_AP_B$.

$$\begin{aligned} c_1 &= m_1 * s_1 \mod p = 7123 \cdot 16723 \mod p = 94527 \mod p, \\ c_2 &= m_2 * s_2 \mod p = 45600 \cdot 84616 \mod p = 64021 \mod p. \end{aligned} \tag{21}$$

Then, the ciphertext is $((8482, 90068), 94527, 64021)$ that is sent to Blain.

After Blain get the message, he first calculate the secret key: $(s_1, s_2) = S_BP_A = (16723, 84616)$

$$\begin{aligned} m_1 &= c_1 * s_1^{-1} \mod p = 94527 \cdot 68665 \mod p = 7123 \mod p, \\ m_2 &= c_2 * s_2^{-1} \mod p = 64021 \cdot 26248 \mod p = 45600 \mod p. \end{aligned} \tag{22}$$

and get the correct keys. Similarly, we can encrypt other parameters and send it to Blain.

5.2. Scrambling process

Assume E refer to the image to be encrypted, take use of (18), the scrambling process can be divided into 4 steps:

1.Assign u_0 to $u(1)$, iterate (18) for $CD-1$ times, ($C \times D$ refer to the size of E), and get $u(i), i = 1, 2, \cdots, CD$.

2.According to the bubble sort, we reorder the $u(i)$ then get $u'(i)$. At the same time, the change of subscript of $u(i)$ is recorded as $z(i)$.

3.Reconstruct $C \times D$ image E into $1 \times CD$ sequence $q(i)$, rank the element of $q(i)$ according to $z(i)$ and get $q'(i)$.

4.Rechange $q'(i)$ into $C \times D$ image denoted by E', which is the permuted image we needed.

The above process is reversible, the permutation can be removed then the plaintext is got.

5.3. Diffusion

1.Do operations described in Section 5.2 and get E'. Change $C \times D$ image E' into $1 \times CD$ sequence $q'(i)$, satisfying $i = B(c-1)+d, (c = 1, 2 \cdots, C, d = 1, 2 \cdots, D)$. Another $C \times D$ image is utilized as a cover image or key image. Change the key image to $1 \times CD$ sequence $k(i)$ by the same way.

2.Set $i = 0$.

3.Round down $u(i) \times 10^4$ as $u_1(i)$, do modular arithmetic between $u_1(i)$and 256 then get

$$u_2(i) \equiv \mod (u_1(i), 256). \tag{23}$$

4.Take the following calculation and get the encrypted pixel value $q''(i)$ by 24:

$$q''(i) = q'(i) \bigoplus \mod (k(i) + u_2(i), 256), \tag{24}$$

here $\bigoplus$ refer to the Xor operation.

The inverse operation of (24) is

$$q'(i) = q''(i) \bigoplus \mod (k(i) + u_2(i), 256). \tag{25}$$

5.Calculate the number g by:

$$g(i) = 1 + \mod (q''(i), 256). \tag{26}$$

Then, iterate (18) $g(i)$ times to get $u(i+1)$.

6.Repeat the operations from Step 3 to Step 5 until $i = CD$. Changing $q''(i)$to $C\ timesD$graph E'', $E''$is the encrypted graph we eventually need.

The decryption process can be divided into the following parts:

1.Perform the same steps in the diffusion section, except that (24) is changed to (25).

2.Do inverse operation of Section 5.2 to eliminate the scrambling effect.

Figure 12 and 13 show the process of the algorithm and the S-box, respectively.

The original, encrypted and decrypted images are shown from Figure 14 to Figure20. The algorithm can encrypt all size of rectangular images. The National Institute of Standards and Technology (NIST) test is currently the most popular test for identifying randomness in chaotic sequences.In NIST test, 15 random test methods are used to test the randomness of fractional time series generated by 2D-TFCDM. If P value > 0.0001, the sequence can be considered as a chaotic sequence. Table 1 lists the NIST test results for fractional 2D-TFCDM.

6. Algorithm Analysis

6.1. Key space

In the proposed algorithm, $(u_0, w_0, \gamma, l_1, l_2, l_3)$ are used as the key, so there are six keys.

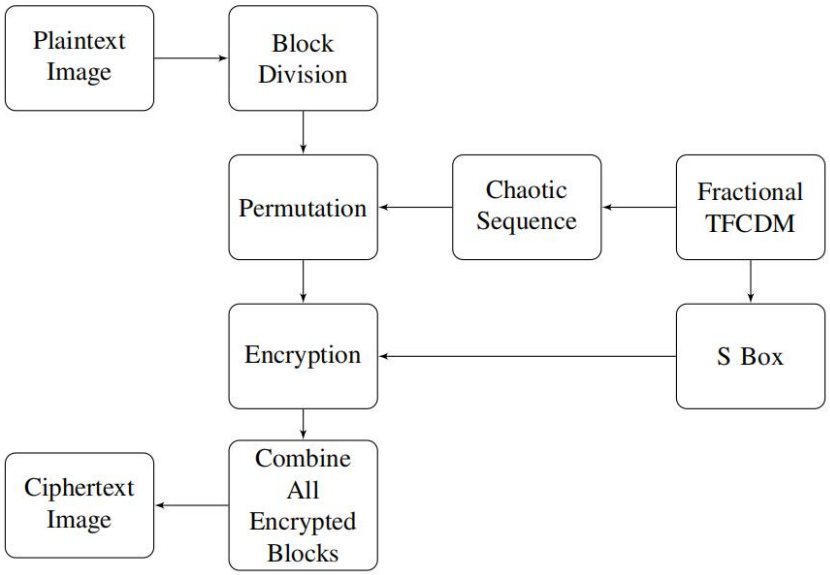


Figure 12: Encryption process.

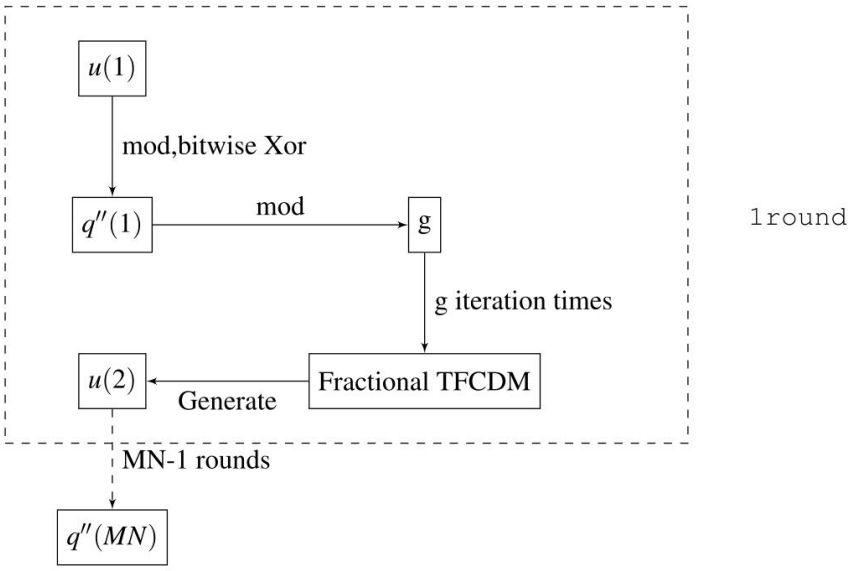
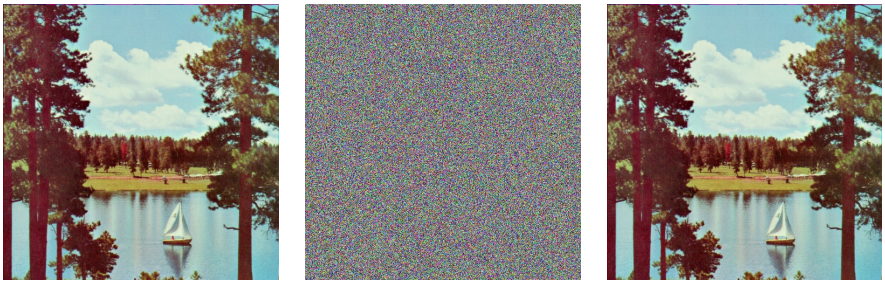


Figure 13: S Box.

Table 1: The NIST test for the chaotic bit Streams

Test	P-VALUE	Pass or not
Frequency	0.739918	√
Block Frequency	0.534146	√
Cumulative Sums forward	0.122325	√
Cumulative Sums reverse	0.739918	√
Runs	0.739918	√
Longest Run	0.213309	√
Rank	0.350485	√
FFT	0.534146	√
Overlapping Template	0.350485	√
Approximate Entropy	0.534146	√
Serial	0.739918	√
Serial	0.534146	√
Linear Complexity	0.739918	√

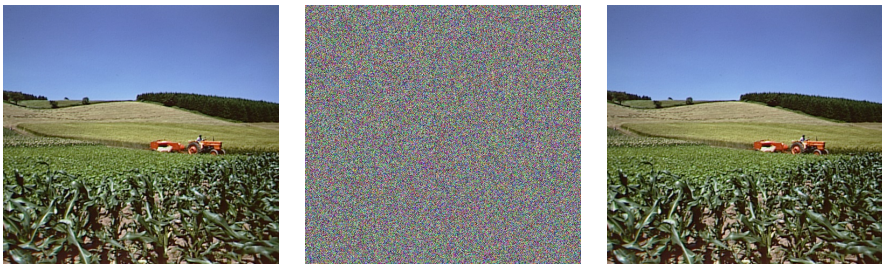


(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 14: Sailboat

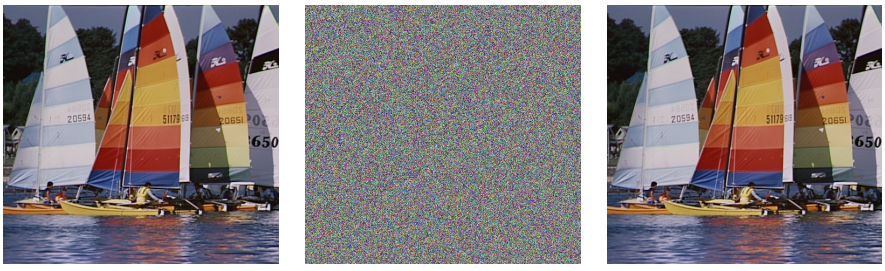
(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 15: Fruits



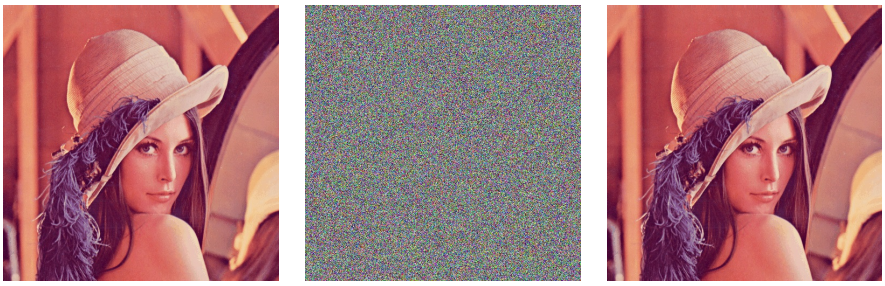
(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 16: Cornfield



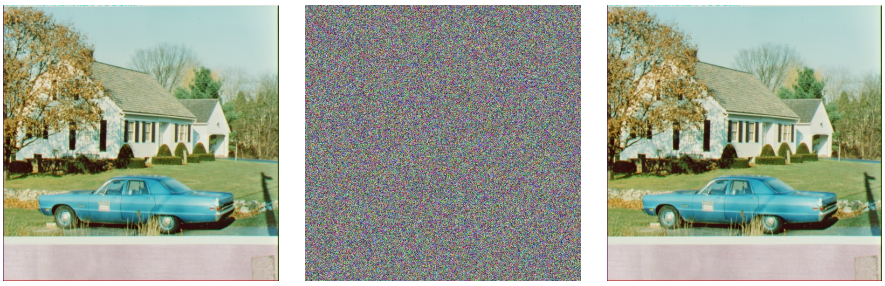
(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 17: Yacht



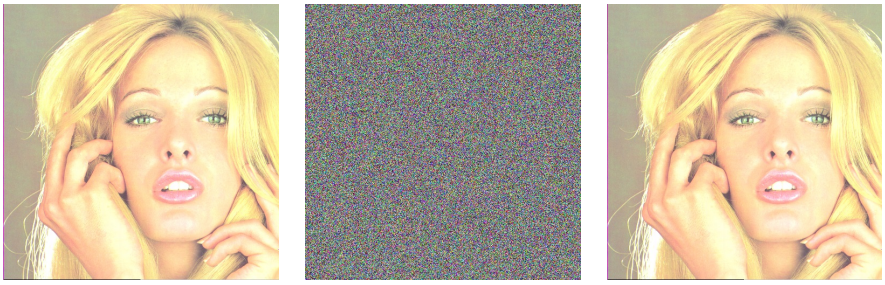
(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 18: Lena



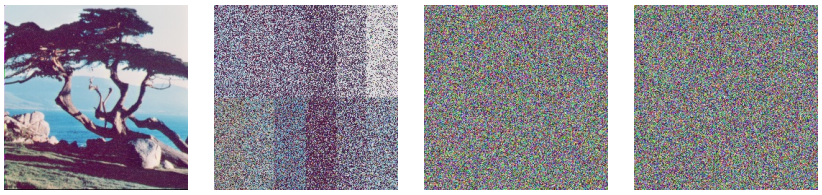
(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 19: House

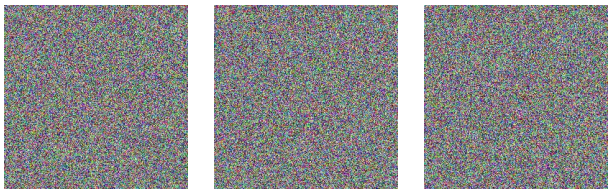


(a) The plaintext (b) The ciphertext (c) The decrypted image

Figure 20: Tiffany



(a) The correct keys (b) $u_0 + 10^{-14}$ (c) $w_0 + 10^{-17}$ (d) $\gamma + 10^{-16}$



(e) $l_1 + 10^{-16}$ (f) $l_2 + 10^{-16}$ (g) $l_3 + 10^{-15}$

Figure 21: The test of Key sensitivity

Table 2: Comparison of key spaces

Algorithm	Ours	[32](2020)	[28](2020)	[20](2022)
Key spaces	$\geq 2.69 \times 10^{102}(1.20 \times 2^{340})$	10^{84}	2^{128}	$> 2^{300}$

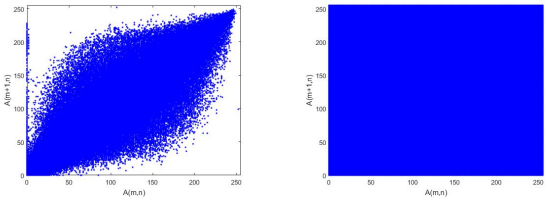
In the key space test, we add $10^{-14}, 10^{-17}, 10^{-16}, 10^{-16}, 10^{-16}, 10^{-15}$ in $u_0, w_0, \gamma, l_1, l_2$ respectively to recover the ciphertext and show it in Figure 21.

As Figure 21 shows, the secret key's space $\geq 10^{14} \times 10^{17} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{15} = 10^{94} \approx 1.20 \times 2^{312}$. If we choose 1024×1024 plaintext, the cover image's key space is $1024 \times 1024 \times 2^8 = 2^{28}$.Therefore, the algorithm key space is $\geq 1.20 \times 2^{340}$. Obviously, our key space is larger than other cases.

6.2. Statistics analysis

The statistical characteristics of ciphertexts are of great significance to ciphertexts. A well-designed encryption method should be able to withstand any statistical attack.

6.2.1. Correlation coefficients(CCs)



(a) The plaintext (b) The ciphertext

Figure 22: Correlation of the Sailboat (in X directions)

The correlation of image pixels is a key index to evaluate the quality of an algorithm. A good encryption algorithm should make the correlation between adjacent pixel values as close to zero as possible.

In equation (27), the CCs are calculated in the vertical, Horizonal and Catercorner directions. The result is shown in Table 3. The correlation in X direction of sailboat before and after the encryption are shown in Figure 22, respectively. The result of other six cases is similar and omitted.

$$r_{uw} = \frac{|cov(u,w)|}{\sqrt{D(u)}\sqrt{D(w)}} \tag{27}$$

$$cov(u,w) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))(w_i - E(w)) \tag{28}$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N}u_i \tag{29}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u)))^2 \tag{30}$$

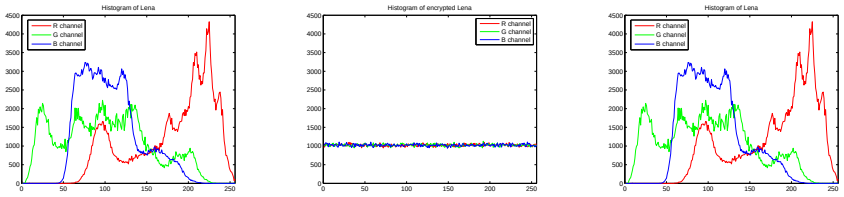
From Figure 22, the correlation of the plaintext is linear, while the correlation of the ciphertext is random. The CCs of the ciphertext is close to 0 in Table 3. The CCs of the plaintexts were all greater than 0.9, and some were close to 1. As can be seen from the statistics in Table 4, most of the CCs of the ciphertext are closer to 0 than other works. Therefore, the proposed algorithm has more advantages than other algorithms.

Table 3: The results of CCs

Image		Lena			Tiffany		
		R	G	B	R	G	B
Plaintext	Horizonal	0.9734	0.9689	0.9391	$-4 * 10^{-5}$	-0.0353	0.0087
	Catercorner	0.9635	0.9495	0.9169	0.0080	-0.0079	0.0073
	Vertical	0.9864	0.9795	0.9568	-0.0266	-0.0046	-0.0061
Ciphertext	Horizonal	0.9505	0.9189	0.9184	0.0176	0.0155	0.0180
	Catercorner	0.9069	0.8641	0.8701	-0.0072	0.0135	-0.0123
	Vertical	0.9427	0.9510	0.9324	-0.0168	-0.0009	0.0090

Table 4: Comparison of CCs for image Lena

Algorithm	plaintext			ciphertext		
	Horizonal	Vertical	Catercorner	Horizonal	Vertical	Catercorner
Ours	0.9391	0.9568	0.9169	0.0087	-0.0061	0.0073
[17](2022)	0.9859	0.9741	0.9618	0.0052	0.0112	0.0034
[15](2021)	0.9775			-0.0379		
[29](2020)	0.9696	0.9151	0.9413	-0.0061	0.0062	0.0014
[30](2020)	0.946	0.921	0.973	-0.0082	0.0007	-0.0059



(a) The plaintext (b) The ciphertext (c) The recovered image

Figure 23: Sailboat

6.2.2. Histogram

The color distribution inside the image is represented with a histogram. Because the unencrypted image has regular color distribution, the attacker can get useful information with the plaintext. Therefore, in a good image encryption method, the ciphertexts should be evenly distributed. Figure 23 is the variation of R,G and B channel in histogram of the Sailboat.

The ciphertext histogram is flat as the ground, while the plaintext is hilly. Obviously, the algorithm has good encryption effect. In the other six cases, the changes could also be like sailboats while the results is omitted.

6.2.3. Information entropy (IE)

Information entropy (IE) is used to express the uncertainty degree of the image. It is defined below:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) log_2 \frac{1}{p(m_i)}, \tag{31}$$

with $p(m_i)$ represents the symbol m_i probability, and n is the needed number of bits to represent the symbol. For images with pixel values between $0 \sim 255$, the ideal IE of an ideal random image is 8 bits according to equation (31). The ciphertext IE in Table 5 show that the ciphertext is very encrypted. According to the Table 6, the proposed algorithm is better than other algorithms.

Table 5: IE

Image		Plaintext	Ciphertext	Image		Plaintext	Ciphertext
Sailboat	R	7.3124	7.9993	Fruits	R	7.5172	7.9992
	G	7.6461	7.9992		G	7.3230	7.9993
	B	7.2137	7.9993		B	6.7785	7.9993
Cornfield	R	7.3115	7.9992	Yacht	R	7.6071	7.9993
	G	7.3550	7.9991		G	7.5386	7.9993
	B	7.6922	7.9992		B	7.6122	7.9992
Lena	R	5.0465	7.9993	House	R	7.4156	7.9993
	G	5.4576	7.9993		G	7.2295	7.9993
	B	4.8001	7.9993		B	7.4354	7.9992
Tiffany	R	4.3374	7.9993				
	G	6.6900	7.9993				
	B	6.4289	7.9992				

Table 6: Comparison of IE

Algorithm	Image	Plaintext	Ciphertext
Ours	Lena	5.0465	7.9993
[20](2022)	Lena	Undefined	7.99227
[15](2021)	Lena	7.6501	7.0562
[17](2022)	Lena	7.4464	7.9973
[19](2021)	Lena	7.3147	7.9976

6.3. Sensitivity

Number of Pixels Change Rate (NPCR) and Unified Average Change Intensity (UACI) are defined to measure the different ranges between two images (33-34):

$$E(i,j) = \begin{cases} 0, I_1(i,j) = I_2(i,j) \\ 1, I_1(i,j) \neq I_2(i,j). \end{cases} \tag{32}$$

$$NPCR = \frac{\sum_{i=1}^{Wt} \sum_{j=1}^{Ht} E(i,j)}{Wt \times Ht} \times 100\% \tag{33}$$

$$UACI = \frac{\sum_{i=1}^{Wt} \sum_{j=1}^{Ht} |I_1(i,j) - I_2(i,j)|}{255 \times Wt \times Ht} \times 100\% \tag{34}$$

Where $Wt \times Ht$ represent the size of the image, respectively. $I_1$and I_2represent the two images analyzed.

6.3.1. Key sensitivity

By use of the key $u_0 = 0.19$, $w_0 = 0.06$, $\gamma = 0.7123456$, $l_1 = 6$ and $l_2 = 2$, we encrypt the image. Figure 21(a) shows the image decrypted with the correct key. Figure 21(b) shows that we decrypt the image with $u_0 + 10^{-14}$, but other keys unchanged. Also, the cases of $\gamma + 10^{-16}, l_1 + 10^{-16}, l_2 + 10^{-16}, w_0 + 10^{-17}$ and $l_3 + 10^{-15}$ respectively with other keys unchanged to decrypt the ciphertext are shown in Figure 21(c-g). Table 2 compare the key spaces between our algorithm with other algorithms. On the other hand, the NPCR and UACI between Figure 21(a) and Figure 21(b-g) are calculated in Table 7 respectively to reflect the difference between them.

The results show that the encryption algorithm is extremely sensitive to the key.

6.3.2. Plaintext sensitivity

A well designed encryption algorithm should have strong plaintext sensitivity, namely it can mainly resist difference attrack. Figure 14(a)(x, y) represents the pixel is changed in Figure 14(a) in (x, y). We encrypt Figure 14(a)(x, y)

Table 7: Key sensitivity

Calculation results between Figure 21(a) and Figure 21(b-g)		
Figure	NPCR(%)	UACI(%)
Figure 21(b)	98.36	26.56
Figure 21(c)	99.62	31.85
Figure 21(d)	99.60	31.92
Figure 21(e)	99.61	32.00
Figure 21(f)	99.62	31.89
Figure 21(g)	99.63	31.97

Table 8: Sailboat

Plaintext sensitivity				
Figure	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 14(a)(30,30)	95.42	32.11	99.60	33.49
Figure 14(a)(50,50)	94.60	31.78	99.59	33.48
Figure 14(a)(80,80)	96.86	32.57	99.59	33.42
Figure 14(a)(100,100)	99.50	33.44	99.60	33.46

and Figure 14(a) at the time, then the UACI and NPCR between the two ciphertexts are calculated and shown in Table 8.

From Table 15, the NPCR of our algorithm is closer to the ideal values 99.61% and the UACI is closer to the ideal values 33.46% than other algorithms [42].

6.4. Selected-plaintext and known-plaintext attacks analysis

From the diffusion in Section 5.3, the current iteration time is determined by the pixel of the ciphertext of the previous round. That is to say, produced by fractional order 2D-TFCDM in (18), $u_2(i)$ depends on the number of iterations $g(i-1)$, and determine the number of iterations $g(i)$.

Therefore, when different plaintexts are encrypted, the corresponding key

Table 9: Fruits

Plaintext sensitivity				
Figure	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 15(a)(30,30)	97.22	32.73	99.61	33.49
Figure 15(a)(50,50)	94.23	31.69	99.60	33.41
Figure 15(a)(80,80)	4.67	1.57	99.61	33.48
Figure 15(a)(100,100)	93.64	31.50	99.61	33.45

Table 10: Cornfield

Plaintext sensitivity				
Figure	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 16(a)(30,30)	97.23	32.66	99.61	33.50
Figure 16(a)(50,50)	94.24	31.66	99.60	33.43
Figure 16(a)(80,80)	5.17	1.73	99.61	33.43
Figure 16(a)(100,100)	93.66	31.48	99.60	33.44

Table 11: Yacht

Plaintext sensitivity				
Figure	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 17(a)(30,30)	97.22	32.65	99.61	33.48
Figure 17(a)(50,50)	94.24	31.68	99.62	33.40
Figure 17(a)(80,80)	99.12	33.28	99.61	33.45
Figure 17(a)(100,100)	93.65	31.46	99.59	33.42

Table 12: Lena

Plaintext sensitivity				
Figure	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 18(a)(30,30)	95.43	32.09	99.62	33.48
Figure 18(a)(50,50)	94.58	31.82	99.61	33.42
Figure 18(a)(80,80)	96.85	32.61	99.61	33.43
Figure 18(a)(100,100)	99.50	33.44	99.59	33.41

Table 13: House

Plaintext sensitivity				
Figure	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 19(a)(30,30)	95.43	32.12	99.60	33.43
Figure 19(a)(50,50)	94.58	31.81	99.61	33.47
Figure 19(a)(80,80)	96.87	32.57	99.61	33.47
Figure 19(a)(100,100)	99.51	33.43	99.61	33.51

Table 14: Tiffany

Plaintext sensitivity				
Image	NPCR(1st)	UACI(1st)	NPCR(2nd)	UACI(2nd)
Figure 20(a)(30,30)	95.41	32.10	99.61	33.47
Figure 20(a)(50,50)	94.59	31.85	99.61	33.47
Figure 20(a)(80,80)	96.87	32.58	99.61	33.47
Figure 20(a)(100,100)	98.24	33.03	99.60	33.49

Table 15: Comparison for plaintext sensitivity with image Lena

Algorithm	NPCR(%)	UACI(%)
Ours	99.61	33.44
[17] (2022)	99.63	33.60
[19](2021)	99.630	33.473
[20](2022)	99.6182	33.4472

Table 16: the NIST test

Test	P-VALUE	Pass or not
Frequency	0.350485	√
Block Frequency	0.911413	√
Cumulative Sums forward	0.350485	√
Cumulative Sums reverse	0.534146	√
Runs	0.213309	√
Longest Run	0.213309	√
Rank	0.991468	√
FFT	0.911413	√
Overlapping Template	0.066882	√
Approximate Entropy	0.534146	√
Serial	0.534146	√
Serial	0.213309	√
Linear Complexity	0.534146	√

streams are different. By Selected-plaintext and known-plaintext attacks, the attacker can't break up the encryption algorithm because the generated pixel value is related to the selected image. Therefore, the proposed attack [43, 44, 45, 46] have no effect on our algorithm.

6.5. Randomness test

Currently, the randomness of ciphertext is tested by NIST tests. We do 15 NIST tests for the ciphered image and show the test results in Table 16. As a conclusion, the ciphertext performs randomness well.

7. Conclusions

Fractional discrete 2D-TFCDM is proposed by discrete fractional calculus. Then, the dynamic behavior is discovered by the proposed map. In addition, the map can also be used in information encryption algorithm. After comparison, the proposed algorithm outperforms other algorithms in almost all aspects.To the best of our knowledge, the proposed color image encryption method has never been reported.

Acknowledgment

The Project was supported by the Natural Science Foundation of Shaanxi Province, China(Grant No. 2021JQ-131), the Fundamental Research Program of Shanxi Province(Grant no. 202103021224317) and the National Natural Science Foundation of China (Grant No. 11975145)

References

[1] K. S. Miller and B. Ross, Fractional difference calculus: Proceedings of the international symposium on univalent functions, fractional calculus and their applications. (1988) 139-152.

[2] M. Bohner and A. Peterson, Dynamic equations on time scales: An introduction with applications, Springer Science & Business Media. (2012).

[3] F.M. Atici, P.W. Eloe, A transform method in discrete fractional calculus, International Journal of Difference Equations, 2 (2007) 165-176.

[4] T.Abdeljawad, D.Baleanu, Fractional differences and integration by parts, journal of computational analysis and applications 13 (2011) 574-582.

[5] F. Chen, X. Luo and Y. Zhou, Existence results for nonlinear fractional difference equation, Advances in Difference Equations, 1 (2011) 1-12.

[6] M. T. Holm, The Laplace transform in discrete fractional calculus, Comput.Math.Appl. 62 (2011) 1591-1601.

[7] Manuel Duarte. Ortigueira, Introduction to fractional linear systems. Part 2: discrete-time case, IEE Proceedings-Vision, Image and Signal Processing. 147 (2000) 71-78.

[8] Manuel D. Ortigueira, Fernando JV Coito, and Juan J. Trujillo, A new look into the discrete-time fractional calculus: derivatives and exponentials, IFAC Proceedings 46 (2013) 629-634.

[9] G. C. Wu , D. Q. Zeng , D. Baleanu. Fractional impulsive differential equations: exact solutions, integral equations and short memory case. Fractional Calculus and Applied Analysis, 22 (1) (2019) 180-192.

[10] G.C.Wu, Z.G. Deng, D. Baleanu, D. Q. Zeng, New variable-order fractional chaotic systems for fast image encryption, Chaos 29 (2019) 083103.

[11] Azil S, Odibat Z, Shawagfeh N. On the dynamics of a Caputo-like discrete fractional Rossler system: chaos, stabilization and synchronization. Physica Scripta, 2022.

[12] Ouannas A, Khennaoui A A, Odibat Z, Pham V T, Grassi G. On the dynamics, control and synchronization of fractional-order Ikeda map. Chaos, Solitons & Fractals, 2019, 123: 108-115.

[13] Ouannas A, Khennaoui A A, Momani S, et al. The discrete fractional duffing system: Chaos, 0C1 test, C 0 complexity, entropy, and control. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2020, 30(8): 083131.

[14] Khennaoui A A, Ouannas A, Odibat Z, et al. On the three-dimensional fractional-order Hnon map with Lorenz-like attractors. International Journal of Bifurcation and Chaos, 2020, 30(11): 2050217.

[15] Singh R K, Kumar B, Shaw D K, Khan D. A. Level by level image compression-encryption algorithm based on quantum chaos map. Journal of King Saud University-Computer and Information Sciences, 2021, 33(7): 844-851.

[16] He Z Y, Abbes A, Jahanshahi H, et al. Fractional-order discrete-time SIR epidemic model with vaccination: Chaos and complexity. Mathematics, 2022, 10(2): 165.

[17] Zhu L, Jiang D, Ni J, et al. A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. Signal Processing, 2022, 195: 108489.

[18] Ma W Li Z Ma N. Synchronization of discrete fractional-order complex networks with and without unknown topology. Chaos: An Interdisciplinary Journal of Nonlinear Science 2022 32(1): 013112.

[19] L. Chen, Y. Hao, L. Yuan, J. T. Machado, R. Wu, and Z. Alam. Double color image encryption based on fractional order discrete improved Henon map and Rubik's cube transform. Signal Processing: Image Communication, (2021) 116363.

[20] Xu S, Wang X, Ye X. A new fractional-order chaos system of Hopfield neural network and its application in image encryption. Chaos, Solitons & Fractals, 2022, 157: 111889.

[21] H. Fu, G C Wu, G Yang, L. L. Huang. Continuous time random walk to a general fractional FokkerCPlanck equation on fractal media, The European Physical Journal Special Topics, (2021) 1-7.

[22] Fiaz M, Aqeel M, Marwan M, Sabir M. Integer and fractional order analysis of a 3D system and generalization of synchronization for a class of chaotic systems. Chaos, Solitons & Fractals, 2022, 155: 111743.

[23] Barba-Franco J J, Gallegos A, Jaimes-Retegui R, Pisarchik A N. Dynamics of a ring of three fractional-order Duffing oscillators. Chaos, Solitons & Fractals, 2022, 155: 111747.

[24] Shi J, He K, Fang H. Chaos, Hopf bifurcation and control of a fractional-order delay financial system. Mathematics and Computers in Simulation, 2022, 194: 348-364.

[25] Haddad I, Belmeguenai A, Herbadji D, et al. Color image encryption based on Fractional-order logistic map//2022 7th International Conference on Image and Signal Processing and their Applications (ISPA). IEEE, 2022: 1-6.

[26] Y.G. Yang, BW Guan, YH Zhou, WM Shi. Double image compression-encryption algorithm based on fractional order hyper chaotic system and DNA approach. Multimedia Tools and Applications, 80 (2021) 691-710.

[27] Li X, Mou J, Cao Y, et al. An optical image encryption algorithm based on a fractional-order laser hyperchaotic system. International Journal of Bifurcation and Chaos, 2022, 32(03): 2250035.

[28] W. S. Sayed, A. G. Radwan, Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems, AEU - International Journal of Electronics and Communications, 123 (2020) 153268.

[29] F Yang, J. Mou, J. Liu, C. Ma, H. Yan, Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application, Signal Processing. 169 (2020) 107373.

[30] L. Ding , Q. Ding. A Novel Image Encryption Scheme Based on 2D Fractional Chaotic Map, DWT and 4D Hyper-chaos. Electronics, 9 (2020) 1280.

[31] M. Z. Talhaoui , X. Wang. A new fractional one dimensional chaotic map and its application in high-speed image encryption. Information Sciences, 550 (2021) 13-26.

[32] S. Li, Y. Yu, X. Ji, Q. Sun. A novel colour image encryption based on fractional order Lorenz system. Systems Science & Control Engineering An Open Access Journal,9 (2020) 1-10.

[33] G.C.Wu, D.Baleanu, Z.X.Lin, Image encryption technique based on fractional chaotic time series, Journal of Vibration and Control. 22 (2016) 2092-2099.

[34] Z. Liu, T. Xia , Wang J. Fractional two-dimensional discrete chaotic map and its applications to the information security with elliptic-curve public key cryptography. Journal of Vibration and Control, 24 (2018) 4797-4824.

[35] Z. Liu, T. Xia , J. Wang, Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem. Chinese Physics B, 27 (2018) 030502.

[36] Z. Liu, T. Xia , Y. Wang, Image Encryption Technology Based on Fractional two Dimensional Discrete Chaotic Map Accompanied with Menezes-Vanstone Elliptic Curve Cryptosystem. Fractals, 29 (2021) 2150064-1152.

[37] Ziad E. Dawahdeh, N. Yaakob. Shahrul, and Razif Bin Othman. Rozmie, A NEW MODIFICATION FOR MENEZES-VANSTONE ELLIPTIC CURVE CRYPTOSYSTEM, Journal of Theoretical and Applied Information Technology, **85**.3 (2016), 290.

[38] Y. Xiao, Research on Elliptic Curve Cryptography, Huazhong University of Science and Technology Press 2006 (in Chinese).

[39] P. Li, L. Min, Y. Hu, G. Zhao, X. Li, Novel two dimensional discrete chaotic maps and simulations, Information and Automation for Sustainability (ICIAfS), 2012 IEEE 6th International Conference on. IEEE, 2012.

[40] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos, 16 (2006) 2129-2151.

[41] C. Li, D. Lin, B. Feng, J. Lv, F. Hao. Cryptanalysis of a Chaotic Image Encryption Algorithm Based on Information Entropy. IEEE Access ,6 (2018) 75834-75842.

[42] F. M. Guo and L. Tu, The application of chaotic theory in cryptography, Beijing Institute of Technology Press. (2015).

[43] D. Xiao, X. Liao, P. Wei. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons & Fractals, 40(5) (2009) 2191-2199.

[44] S.Dhall , S. K. Pal, K. Sharma, Cryptanalysis of image encryption scheme based on a new 1D chaotic system, Signal Processing, 146 (2018) 22-32.

[45] F Yu, X Gong, H. Li, S. Wang. Differential cryptanalysis of image cipher using block-based scrambling and image filtering. Information Sciences, 554 (2021) 145-156 .

[46] I. E. Hanouti, H. E. Fadili, K. Zenkouar. Cryptanalysis of an embedded systems' image encryption. Multimedia Tools and Applications 80(9) (2021) 13801-13820.