Nonlinear Dyn (2024) 112:20437–20459
https://doi.org/10.1007/s11071-024-10083-2

RESEARCH

# Non-degenerate multi-stable discrete chaotic system for image encryption

**Xiaojun Tong · Xudong Liu · Miao Zhang · Zhu Wang · Yunhua Fan**

Received: 13 March 2024 / Accepted: 24 July 2024 / Published online: 1 August 2024

**Abstract** The design of cryptographic algorithms using the chaos theory has become a hotspot in the field of information security. However, existing chaotic systems are prone to chaotic degradation, and generally do not exhibit multi-stability. In view of these issues, we first propose a non-degenerate multi-stable discrete chaotic system (NMDCS). After a rigorous theoretical analysis, it is proved that the NMDCS has an infinite number of unstable fixed points, and the number of positive Lyapunov exponents (LE) is equal to the system dimensions, indicating that the system has an infinite number of coexisting attractors and is not susceptible to chaotic degradation. In addition, Simulation experiments demonstrate that the NMDCS displays significant chaotic behavior and high efficiency. Finally, to satisfy the confidentiality protection demands for sensitive images, an efficient image encryption algorithm is designed by combining the NMDCS with an adaptive zigzag transformation method. Simulation experiments demonstrate that our image encryption algorithm has high efficiency in both encryption and decryption processes. Moreover, it demonstrates excellent security properties.

**Keywords** Chaos · Non-degeneracy · Coexisting attractor · Image encryption

## 1 Introduction

Communication over the globe is becoming a basic need of populaces [1]. However, the inherent openness, dynamism, and complexity of the Internet frequently result in information leakage incidents, which makes it imperative to enhance the security level of sensitive information. The most direct method for the protection of information confidentiality is encryption, and various classic encryption algorithms, such as data encryption standard (DES) and advanced encryption standard (AES), have been proposed successively. Although these algorithms are easily available, extensively tested, and widely accepted for text data encryption, their application in image encryption is constrained due to the large amount of data, strong correlation between adjacent pixels, and high redundancy of image data.

Chaos is a central research topic of nonlinear theories. It exhibits distinctive properties, including initial state sensitivity, topological transitivity, and periodic orbit density [2]. These properties establish a natural connection between chaos and traditional cryptography, resulting in wide application in various fields such

X. Tong · X. Liu (✉) · M. Zhang
School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China
e-mail: liuxd_work@163.com

Z. Wang
School of Information and Electrical Engineering, Harbin Institute of Technology, Weihai 264209, China

Y. Fan
Digital Research Branch of Inner Mongolia Power (Group) Co., Ltd, Hohhot 010000, China

as S-box design [3,4] and information hiding [5,6]. At present, more than 32% of image encryption algorithms are designed based on chaos theory. Chaotic image encryption algorithms offer confidentiality protection for sensitive images in a variety of fields, such as e-medicine, military reconnaissance, remote sensing mapping, etc., thus avoiding the security risks associated with leaks of private information and misuse of data.

The fundamental prerequisite for the design of chaotic image encryption algorithms is the establishment of chaotic systems with excellent dynamic behavior. Chaotic systems are classified into two types: continuous chaotic systems and discrete chaotic systems. Currently, researchers mainly focus on continuous chaotic systems. For example, Yang et al. [7] designed a fractional-order hyperchaotic system based on the Lorenz system and analyzed the dynamical behavior of this system in detail using the Adomian decomposition method. Ma et al. [8] presented a multi-stable chaotic system with coexisting attractors by tuning the offset operation. However, continuous chaotic systems are inefficient due to the necessity of using time-consuming numerical analysis methods, like the Runge–Kutta method or the Adomian decomposition method, to generate chaotic sequences [9]. Discrete chaotic systems have proven to be more efficient than continuous chaotic systems, and a variety of classical chaotic maps, such as the Logistic map and the Tent map, have been successively introduced. However, Hua et al. [10] pointed out that the structure of these chaotic maps is relatively simple. In general, high-dimensional discrete chaotic systems are more likely to produce hyperchaotic attractors, which implies better chaotic properties. Choi et al. [11] constructed generalized high-dimensional Arnold systems using the Laplace theorem. Hua et al. [12] constructed high-dimensional discrete chaotic systems by composing classical low-dimensional discrete chaotic systems. Through rigorous theoretical analysis, Liu et al. [13] demonstrated that the third-order nonlinear filter can exhibit strong chaotic behavior if its system parameters are chosen appropriately. Unfortunately, the limited number of positive LE in the mentioned discrete chaotic systems is significantly lower than their dimensions, making them susceptible to chaotic degradation during digitization. To tackle this issue, Hua et al. [14] first discussed the internal relationship between the number of positive LE and the Arnold parameter matrix. Then, they presented a high-dimensional discrete chaotic system with an arbitrary number of positive LE. Wang et al. [15] and Zang et al. [16] designed non-degenerate discrete chaotic systems by using the chaotic inverse control method and the strict diagonal occupation matrix respectively. Liu et al. [17] also proposed a non-degenerate discrete chaotic system with uniform trajectories using nonlinear filters and the feed-forward and feed-back structure. Since the above discrete chaotic systems have a much greater number of positive LE compared to general chaotic systems, they are capable of displaying complex chaotic behavior. However, these systems do not exhibit multi-stability, which means that they are unable to switch freely between various steady states to meet diverse demands. Qin [18] pointed out that chaotic systems with more equilibrium points may contain more attractors, resulting in different coexisting attractors. Due to the inherent nonlinearity and periodicity of trigonometric functions, researchers have recently begun to investigate the design of multi-stable chaotic systems using them [19]. For example, Ali et al. [20] constructed a novel chaotic map using two sine functions with irrational frequency ratios but comparable amplitude and phase, and found coexisting attractors. Huang et al. [21] proposed a three-dimensional (3D) multi-stable hyperchaotic map with a concise symmetric structure. Furthermore, memristors are employed to enhance the dynamic behavior of multi-stable chaotic systems due to their distinctive nonlinear characteristics [22]. Ma et al. [23] designed a memristive chaotic system that has infinite equilibrium points and can exhibit seven different types of attractors. Liu et al. [24] and Marco et al. [25] proposed a class of discrete multi-stable chaotic systems using discrete memristors, respectively. However, these chaotic systems do not meet the non-degeneracy requirement and remain susceptible to chaotic degradation.

Chaos theory offers a plethora of beneficial insights for the design of image encryption algorithms. In 1989, Matthews et al. put forward the first chaotic image encryption algorithm using the Logistic map. Subsequently, Li et al. [26] constructed a key stream generator using the Tent map and applied it to the design of a stream cipher algorithm that is suitable for image confidentiality protection. Sang et al. [27] generated cipher images with excellent statistical features by scrambling plain images using the Logistic map and incorporating uniform distribution constraints to the training of deep auto-encoder. However, the above image encryption algorithms suffer from potential security risks due to the simple structure of the chaotic maps they use. In response to the above problem, Lai et al. [28] designed a novel neuron model with significant chaotic properties and applied it to the design of image encryption algorithms. Wang et al. [29] first designed a hyperchaotic system with complex chaotic behavior based on the Lorenz system and then proposed a color image encryption algorithm by combining the chaotic system and deoxyribonucleic acid (DNA) coding. Hua et al. [30] put forward an image encryption algorithm using a novel Logistic-Sine-coupling chaotic system. Javeed et al. [31] put forward an image encryption algorithm using the Rabinovich-Fabricant chaotic system. The above research has contributed to the research progress in the field of chaotic image encryption. However, none of the above chaotic systems are non-degeneracy, which may lead to security risks in image encryption algorithms due to chaotic degradation. To overcome this drawback, Wen et al. [32] and Wang et al. [33] proposed plaintext-related chaotic image encryption algorithms using non-degenerate discrete chaotic systems and the hash values of plain images, respectively. However, the derived key in the above algorithm is strongly linked to the hash values of plain images, making even a slight alteration in the hash value during transmission could result in decryption failure. Thus, how to securely transmit the hash value of a plain image limits the application of such image encryption algorithms.

Although chaotic cryptography has achieved several important research results after years of development, the existing chaotic systems are susceptible to chaotic degradation and generally do not exhibit multi-stability, and the current chaotic image encryption algorithms suffer from low efficiency in encryption and decryption and inadequate security measures. As such, existing research faces challenges in meeting the criteria for safeguarding the confidentiality of sensitive images In conclusion, there is still considerable research value in investigating non-degenerate multi-stable discrete chaotic systems and applying them to the design of effective image encryption algorithms.

The remainder of this paper is structured as follows. Section 2 presents a non-degenerate multi-stable discrete chaotic system that is analyzed through theoretical analysis and simulation experiments. In Sect. 3, we propose an image encryption algorithm based on non-degenerate multi-stable discrete chaos, and its performance is evaluated. Section 4 concludes this paper.

## 2 Non-degenerate multi-stable discrete chaotic system

In this section, we design a discrete chaotic system called NMDCS. Rigorous theoretical analyses and simulation experiments demonstrate that the NMDCS exhibits multi-stability and is not prone to chaotic degradation.

### 2.1 Mathematical expression of our discrete chaotic system

The mathematical model of $N$-dimensional NMDCS is described by Eq. (1), whose block diagram is shown in Fig. 1.

$$\begin{cases} x_{1,t+1} = \sin\left(\pi \cdot x_{2,t}\right) \\ \vdots \\ x_{N-1,t+1} = \sin\left(\pi \cdot x_{N,t}\right) \\ x_{N,t+1} = x_{N,t} + \sin\left(\pi \cdot x_{1,t}\right) - \frac{a}{\pi} \cdot \sin\left(\frac{\pi \cdot x_{N,t}}{a}\right) \end{cases} \tag{1}$$

where $a = \frac{b}{2 \cdot c}$ is the system parameter, $b, c \in \mathbb{Z} \setminus \{0\}$ are coprime, $|b| > 6 \cdot |c|$, $\left\{x_{1,t}, x_{2,t}, \cdots, x_{N-1,t}\right\} \in I$ and $x_{N,t} \in I^*$ are the chaotic state variables at moment $t$, $I = [-1, 1]$ and $I^* = [-1+k \cdot b+\varepsilon_1, 1+k \cdot b+\varepsilon_2]$ are the chaotic intervals, $k \in \mathbb{Z}$, and the absolute values of $\varepsilon_1$ and $\varepsilon_2$ are far less than 1.

### 2.2 Theoretical analysis of our discrete chaotic system

In this section, we prove that the NMDCS system has unstable fixed points, and is not susceptible to chaotic degradation.

#### *2.2.1 Fixed points analysis*

According to Eq. (1), the fixed point equation of our NMDCS system can be derived as Eq. (2).

$$\begin{cases} x_{1.t} = \sin\left(\pi \cdot x_{2.t}\right) \\ \vdots \\ x_{N-1.t} = \sin\left(\pi \cdot x_{N.t}\right) \\ x_{N.t} = x_{N.t} + \sin\left(\pi \cdot x_{1.t}\right) - \frac{a}{\pi} \cdot \sin\left(\frac{\pi \cdot x_{N.t}}{a}\right) \end{cases} \tag{2}$$

Obviously, Eq. (2) has an infinite number of solutions. Therefore, the fixed points of the NMDCS system can be expressed as $X = \{0, 0, \cdots, 0, k \cdot b\}$.

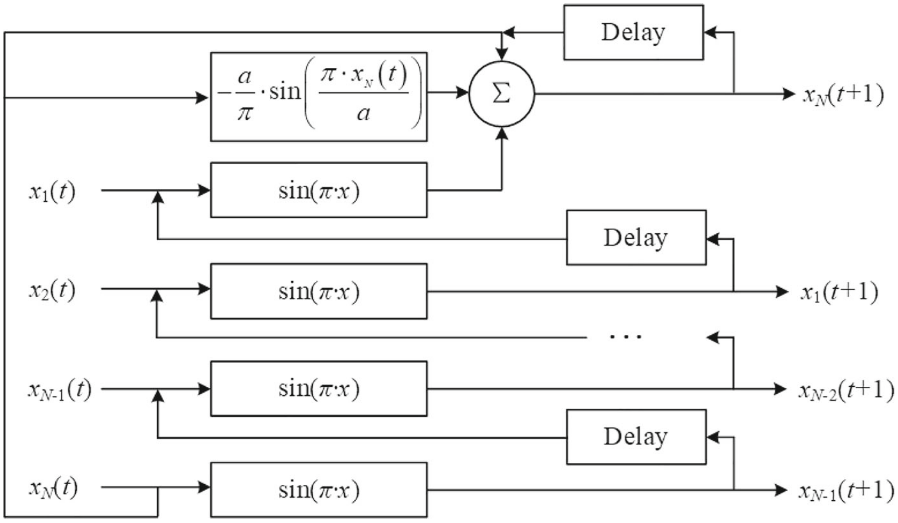


**Fig. 1** Block diagram of NMDCS

The Jacobian matrix of Eq. (2) at $X$ is described by Eq. (3).

$$\mathbf{J}_t = \begin{pmatrix} 0 & \pi & 0 & \cdots & 0 \\ 0 & 0 & \pi & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \pi \cdot \cos(\pi \cdot k \cdot b) \\ \pi & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{3}$$

The characteristic polynomial of Eq. (3) is defined by Eq. (4).

$$g(\lambda_t) = \lambda_t^N + (-\pi)^N \cdot \cos(\pi \cdot k \cdot b) \tag{4}$$

According to Eq. (4), we can derive the eigenvalues as Eq. (5).

$$\lambda_t = -\pi \cdot e^{\frac{i\cdot\pi\cdot(k\cdot b+1)}{N}} \tag{5}$$

where $i^2 = -1$.

It is clear that there must be eigenvalues with zero or positive real parts, which means that the fixed point $X$ may be critically stable or unstable.

### *2.2.2 Non-degenerate analysis*

In this section, we analyze the trajectories of our NMDCS system using the following lemmas. Afterwards, we prove that the NMDCS system is a non-degenerate chaotic system using the above lemmas.

**Lemma 1** *If $x_{n,0}$ follows the uniform distribution in the interval I, the probability density function of $x_{n,1} = f(x_{n,0}) = \sin(\pi \cdot x_{n,0})$ can be derived as $p(x_{n,1}) = \begin{cases} \frac{1}{\pi\sqrt{1-x_{n,1}^2}}, if\, x_{n,1} \in I \\ 0, others \end{cases}$, where $n \in \{1, 2, \ldots, N\}$.*

*Proof* Since $x_{n,0}$ follows the uniform distribution in the interval $I$, its probability density function is $p(x_{n,0}) = \begin{cases} \frac{1}{2}, if\, x_{n,0} \in I \\ 0, others \end{cases}$. Divide the interval $I$ into a series of subintervals $I_l = \left[\frac{l-1}{2}, \frac{l}{2}\right)$, where $l \in \{-1, 0, 1, 2\}$. Let $h(x_{n,1})$ be the inverse function of $f(x_{n,0})$, whose expression is shown in Eq. (6).

$$h(x_{n,1}) = \begin{cases} \frac{\arcsin(x_{n,1})}{\pi}, if\, x_{n,0} \in I_0 \cup I_1 \\ -\frac{\arcsin(x_{n,1})}{\pi} \mp 1, if\, x_{n,0} \in I_{-1} \cup I_2 \\ 0, others \end{cases} \tag{6}$$

According to Eq. (6), the probability density function of $x_{n,1} = f(x_{n,0})$ can be derived as Eq. (7).

$$\begin{aligned} p(x_{n,1}) &= \begin{cases} p(h(x_{n,1})) \cdot \left|h'(x_{n,1})\right|, if\, x_{n,1} \in I \\ 0, others \end{cases} \\ &= \begin{cases} \sum_{l=-1,0} \frac{1}{2} \cdot \left|(-1)^l \cdot \frac{1}{\pi\sqrt{1-x_{n,1}^2}}\right|, if\, x_{n,1} \in I_{-1} \cup I_0 \\ \sum_{l=1,2} \frac{1}{2} \cdot \left|(-1)^{l-1} \cdot \frac{1}{\pi\sqrt{1-x_{n,1}^2}}\right|, if\, x_{n,1} \in I_1 \cup I_2 \\ 0, others \end{cases} \\ &= \begin{cases} \frac{1}{\pi\sqrt{1-x_{n,1}^2}}, if\, x_{n,1} \in I \\ 0, others \end{cases} \end{aligned} \tag{7}$$

Lemma 1 is thus proved. □

**Lemma 2** *If $x_{n,0}$ follows the uniform distribution in the interval $I$, the probability density function of $x_{n,2} = f(f(x_{n,0})) = \sin(\pi \cdot \sin(\pi \cdot x_{n,0}))$ can be derived*

$$as \;\; p\left(x_{n,2}\right) = \begin{cases} \frac{1}{\pi\sqrt{1-x_{n,2}^2}} \cdot \sum_{i=0,1} \\ \frac{1}{\sqrt{\pi^2-(\arcsin|x_{n,2}|-i\cdot\pi)^2}}, if \, x_{n,2} \in I\;, \\ 0, others \end{cases}$$

*where* $n \in \{1, 2, \ldots, N\}$.

*Proof* Divide the interval $I$ into a series of subintervals $I_l = \left[\frac{l-1}{2}, \frac{l}{2}\right)$, where $l \in \{-1, 0, 1, 2\}$. Let $h\left(x_{n,2}\right)$ be the inverse function of $f\left(x_{n,1}\right)$, whose expression is listed in Eq. (8).

$$h\left(x_{n,2}\right) = \begin{cases} \frac{\arcsin(x_{n,2})}{\pi}, if \, x_{n,1} \in I_0 \cup I_1 \\ -\frac{\arcsin(x_{n,2})}{\pi} \mp 1, if \, x_{n,1} \in I_{-1} \cup I_2 \\ 0, others \end{cases} \tag{8}$$

From Eq. (8), the probability density function of $x_{n,2} = f\left(x_{n,1}\right)$ can be derived as Eq. (9).

$$\begin{aligned} p\left(x_{n,2}\right) &= \begin{cases} p\left(h\left(x_{n,2}\right)\right) \cdot \left|h'\left(x_{n,2}\right)\right|, if \, x_{n,2} \in I \\ 0, others \end{cases} \\ &= \begin{cases} \sum_{l=-1,0} \frac{1}{\pi\sqrt{1-x_{n,1}^2}} \cdot \\ \left|(-1)^l \cdot \frac{1}{\pi\sqrt{1-x_{n,2}^2}}\right|, if \, x_{n,2} \in I_{-1} \cup I_0 \\ \sum_{l=1,2} \frac{1}{\pi\sqrt{1-x_{n,1}^2}} \cdot \\ \left|(-1)^{l-1} \cdot \frac{1}{\pi\sqrt{1-x_{n,2}^2}}\right|, if \, x_{n,2} \in I_1 \cup I_2 \\ 0, others \end{cases} \\ &= \begin{cases} \frac{1}{\pi\sqrt{1-x_{n,2}^2}} \cdot \sum_{l=-1,0} \\ \frac{1}{\sqrt{\pi^2-(\arcsin(x_{n,2})-l\cdot\pi)^2}}, if \, x_{n,2} \in I_{-1} \cup I_0 \\ \frac{1}{\pi\sqrt{1-x_{n,2}^2}} \cdot \sum_{l=1,2} \\ \frac{1}{\sqrt{\pi^2-(\arcsin(x_{n,2})-(l-1)\cdot\pi)^2}}, if \, x_{n,2} \in I_1 \cup I_2 \\ 0, others \end{cases} \\ &= \begin{cases} \frac{1}{\pi\sqrt{1-x_{n,2}^2}} \cdot \sum_{i=01} \frac{1}{\sqrt{\pi^2-(\arcsin|x_{n,2}|-i\cdot\pi)^2}}, if \, x_{n,2} \in I \\ 0, others \end{cases} \end{aligned} \tag{9}$$

Lemma 2 is thus proved. □

**Theorem 1** *The NMDCS system is a non-degenerate discrete chaotic system.*

*Proof* From Eq. (1), the Jacobian matrix of the NMDCS system at moment $t$ is shown in Eq. (10).

$$\mathbf{J}_t = \begin{pmatrix} 0 & f'\left(x_{2,t}\right) & 0 & \cdots & 0 \\ 0 & 0 & f'\left(x_{3,t}\right) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & f'\left(x_{N,t}\right) \\ f'\left(x_{1,t}\right) & 0 & 0 & \cdots & 1-\cos\left(\frac{\pi\cdot x_{N,t}}{a}\right) \end{pmatrix} \tag{10}$$

Where $f'\left(x_{n,t}\right) = \pi \cdot \cos\left(\pi \cdot x_{n,t}\right)$ and $n \in \{1, 2, \ldots, N\}$. The characteristic polynomial of (10) can be derived as (11).

$$g\left(\lambda_t\right) = \lambda_t^{N-1} \cdot \left(\lambda_t - 1 + \cos\left(\frac{\pi \cdot x_{N,t}}{a}\right)\right) + (-\pi)^N \cdot \prod_{n=1}^{N} \cos\left(\pi \cdot x_{n,t}\right) \tag{11}$$

As is shown in Sect. 2.1, it is clear that $|a| > 3$. Thus, we can derive Eq. (12) from Eq. (11).

$$g\left(\lambda_t\right) \approx \lambda_t^N + (-\pi)^N \cdot \prod_{n=1}^{N} \cos\left(\pi \cdot x_{n,t}\right) \tag{12}$$

According to Eq. (12), we can derive the eigenvalues as Eq. (13).

$$\left|\lambda_{n,t}\right| = \left|\pi \cdot \cos\left(\pi \cdot x_{n,t}\right)\right| \tag{13}$$

From Eq. (13) and Lemma 2, we can derive the LE of our NMDCS system as $\{LE_1, \cdots, LE_n, \cdots, LE_N\}$, where $LE_n$ is calculated by Eq. (14).

$$\begin{aligned} LE_n &= \int_{-1}^{1} \ln\left|\lambda_{n,t}\right| \cdot p\left(x_{n,t}\right) dx_{n,t} \\ &\approx \int_{-1}^{1} \ln\left|\lambda_{n,2}\right| \cdot p\left(x_{n,2}\right) dx_{n,2} \\ &= 0.6672 \end{aligned} \tag{14}$$

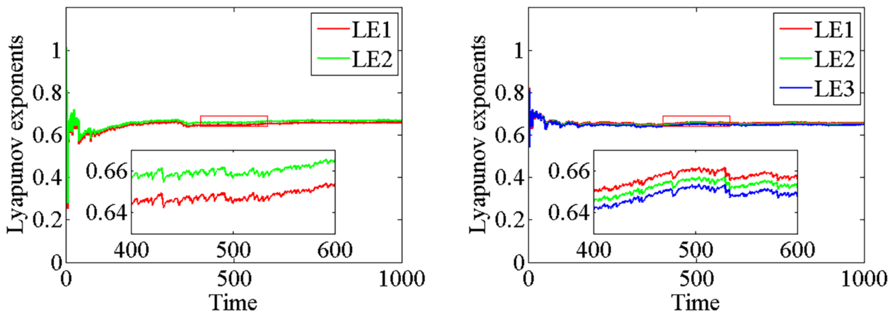
In conclusion, the LE of the NMDCS system are all 0.6672, indicating that our NMDCS system is a non-degenerate discrete chaotic system. □

## 2.3 Simulation experiments of our discrete chaotic system

This section demonstrates that our NMDCS system shows excellent chaotic behavior from the aspects of LE, coexisting attractors, Poincaré section, sensitive dependence on initial conditions, and iterative efficiency. Our experiments were conducted on a Windows machine running on an Intel Core i5-6300HQ and 12 GB RAM.

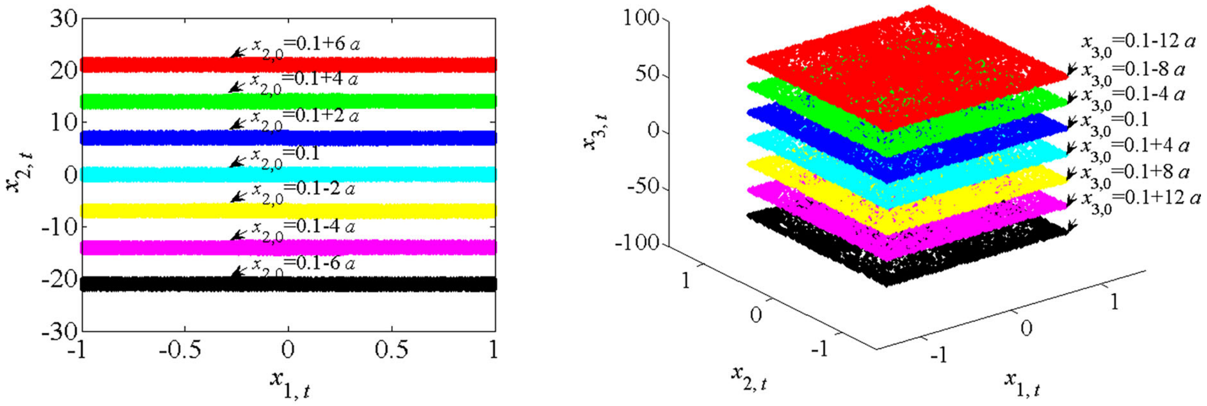
### *2.3.1 Lyapunov exponent spectrum*

LE is always used to measure the rate of convergence or divergence of adjacent trajectories of a dynamical system. A positive LE means that the system stays in a chaotic state. If there are more than two positive LEs, the chaotic map becomes hyper-chaos and



(a) $a = 15/2$, Initial states (-0.1,0.2) (b) $a = -21/4$, Initial states (-0.9,-0.3,0.7)

**Fig. 2** Lyapunov exponent spectrum of our discrete chaotic system



(a) $N = 2$, $a = 7/2$, $x_{1,0} = 0.5$ (b) $N = 3$, $a = -21/4$, $x_{1,0} = 0.3$, $x_{2,0} = 0.5$

**Fig. 3** Coexisting attractors of our discrete chaotic system

exhibits complex chaotic behavior in multiple dimensions. This section conducts simulation experiments to estimate the LE of the NMDCS, and the experimental results are shown in Fig. 2.

As is shown in Fig. 2, the number of positive LE of our NMDCS system is equal to its dimension, regardless of the selection of the system parameter $a$. Additionally, the LE values are all very close to the theoretical value of 0.6672 derived from Theorem 1. Therefore, the NMDCS system is a non-degenerate discrete chaotic system with stronger chaotic behavior than most of the existing chaotic systems, and is not prone to chaotic degradation during digitization.

*2.3.2 Coexisting attractor analysis*

Due to the periodic properties of trigonometric functions, the position of the attractor of the NMDCS system depends on the initial state $x_{N,0}$, which means that our NMDCS system has coexisting attractors. This behavior is very interesting, and next we will draw the phase diagrams of the NMDCS system by selecting different $x_{N,0}$ to understand this phenomenon more intuitively. The simulation results are listed in Fig. 3.

**Table 1** Efficiency comparison results

| Chaotic system | Efficiency (Mbps) |
|---|---|
| Ours | 53.2595 |
| Zang [16] | 64.6367 |
| Qin [18] | 21.3385 |
| Liu [24] | **75.6923** |
| Ye [34] | 18.3195 |
| Yang [35] | 17.2291 |

Bold value indicates the optimal performance of the corresponding test items

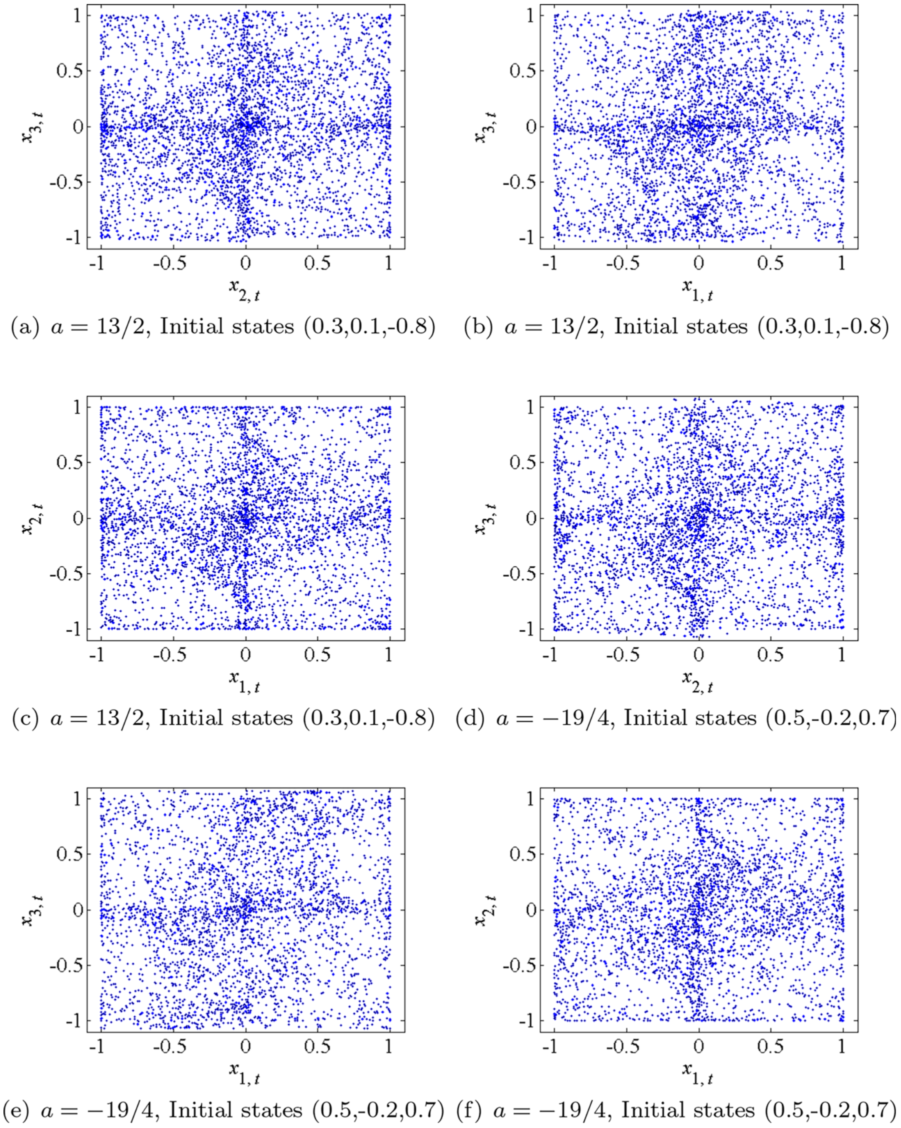
From Fig. 3, it is obvious that the coexisting attractors of the NMDCS system are all square or cube, regardless of the initial state, which means that these coexisting attractors are all homogeneous. This is because although the initial states between different coexisting attractors are completely different, $2a$ and $4a$ are the period of the nonlinear term $\sin\left(\frac{\pi \cdot x_{N,t}}{a}\right)$ in Eq. (1) respectively, so there will be no significant difference in the shape of the coexisting attractors.

### *2.3.3 Efficiency analysis*

Efficiency is a crucial factor in assessing the practicality of chaotic systems. This section examines the effectiveness of chaotic systems through the symbol transfer rate. During the analysis, each chaotic system generated 320 Mbit of chaotic sequences. Table 1 shows the results of the efficiency analysis.

As demonstrated in Table 1, the efficiency of our NMDCS exceeds that of the chaotic systems in [18, 34, 35]. This is because chaotic systems in [18, 34, 35] necessitate the utilization of time-consuming numerical analysis techniques, such as the Runge–Kutta

**Fig. 4** Poincaré sections of our chaotic system

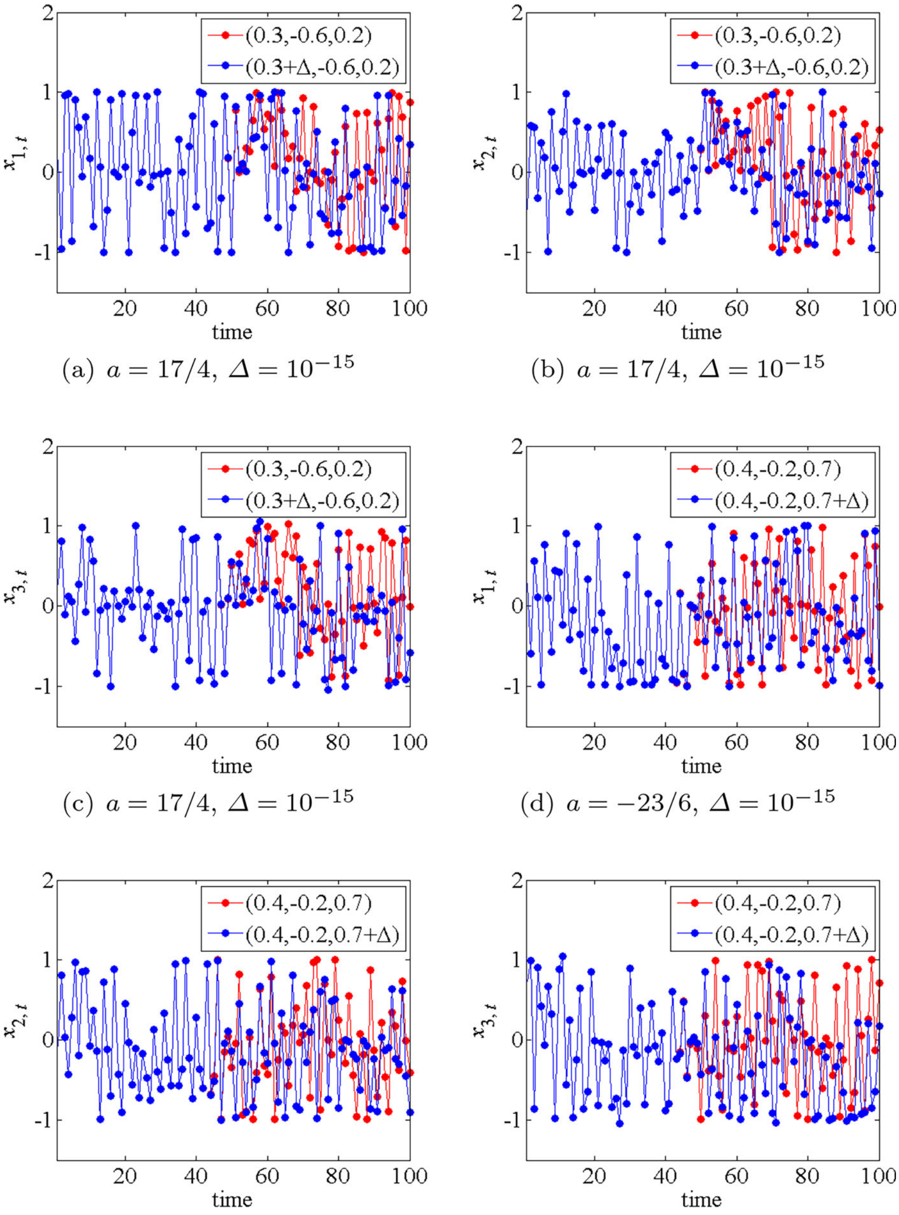


(a) $a = 13/2$, Initial states (0.3,0.1,-0.8) (b) $a = 13/2$, Initial states (0.3,0.1,-0.8)

(c) $a = 13/2$, Initial states (0.3,0.1,-0.8) (d) $a = -19/4$, Initial states (0.5,-0.2,0.7)

(e) $a = -19/4$, Initial states (0.5,-0.2,0.7) (f) $a = -19/4$, Initial states (0.5,-0.2,0.7)

**Fig. 5** Initial state sensitivity of our chaotic system



(a) $a = 17/4,\ \varDelta = 10^{-15}$

(b) $a = 17/4,\ \varDelta = 10^{-15}$

(c) $a = 17/4,\ \varDelta = 10^{-15}$

(d) $a = -23/6,\ \varDelta = 10^{-15}$

(e) $a = -23/6,\ \varDelta = 10^{-15}$

(f) $a = -23/6,\ \varDelta = 10^{-15}$

method, throughout the iterative process. Although the efficiency of the NMDCS may not be on par with the chaotic systems described in [16,24] due to the use of slightly time-consuming trigonometric function operations, it still achieves a symbol transmission rate of 53.2595 Mbps. Therefore, we can conclude that our NMDCS exhibits a commendable level of efficiency.

### *2.3.4 Poincaré section analysis*

The Poincaré section is always used to analyze the dynamical behavior of multivariate autonomous systems. If there are only a few points on the Poincaré section, the motion is periodic. Otherwise, if there is a closed curve on the Poincaré section, the motion is determined to be quasi-periodic. When there are patches of dense points on the Poincaré section, the

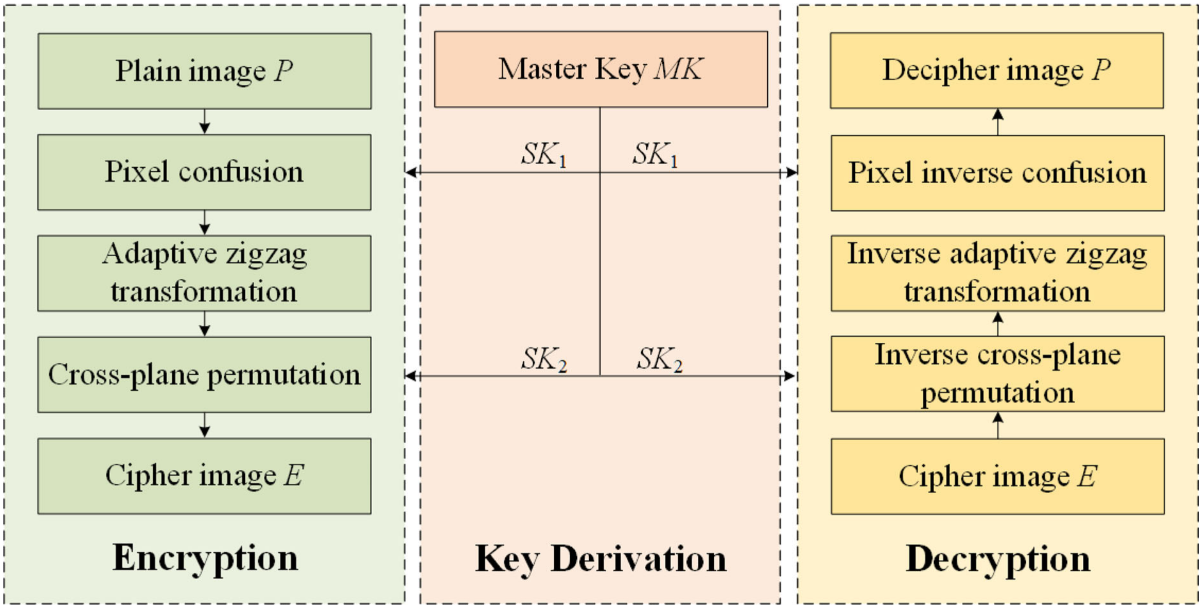


**Fig. 6** Block diagram of IEA-NMDCS

motion is assumed to be chaotic. This section sets various system parameters, and the Poincare section of our NMDCS system is shown in Fig. 4.

As is shown in Fig. 4, it can be seen that although the system parameters of the NMDCS are different, there are patches of dense points distributed on each Poincaré section. The above results further indicate that our NMDCS is chaotic.

#### *2.3.5 Sensitivity to initial conditions*

Initial condition sensitivity is the most essential property of chaotic systems, reflecting the inherent randomness of chaotic systems. Initial condition sensitivity refers to the fact that tiny differences between the initial states of a chaotic system will result in completely different trajectories, indicating that the long-term motion state of a chaotic system is unpredictable. In this section, different system parameters are selected to test the initial condition sensitivity of our NMDCS system, and the results are shown in Fig. 5.

As is shown in Fig. 5, it is obvious that slight changes between the initial values will cause our chaotic system to exhibit completely different trajectories. Therefore, our NMDCS system is highly sensitive to initial conditions and is particularly suitable for the design of cryptographic algorithms.

## 3 Image encryption algorithm based on non-degenerate multi-stable discrete chaos

Since our NMDCS system is not susceptible to chaotic degradation and has an infinite number of coexisting attractors, the chaotic system is used to design an efficient and secure image encryption algorithm.

### 3.1 Overall flow of the algorithm

Our image encryption algorithm based on non-degenerate multi-stable discrete chaos (IEA-NMDCS) mainly involves four steps of key derivation, pixel confusion, adaptive zigzag transformation, and cross-plane permutation, and its block diagram is shown in Fig. 6.

#### *3.1.1 Key derivation*

Our key derivation algorithm takes the 144-bit master key $MK = MK_1 || MK_2 || MK_3$ as input to generate the derived keys $SK_1$, $SK_2$ for subsequent encryption and decryption operations, where the lengths of $MK_1$, $MK_2$, $MK_3$ are all 48-bit, and $||$ represents the link symbol. The procedure of the algorithm is shown in Algorithm 1.

(1) It calculates the chaotic initial state $IV = \{IV_i\}_{i\in\{1,2,3\}}$, where $IV_i = \frac{MK_i}{2^{47}} - 1$.

(2) It generates a chaotic sequence $Q$ of size $R \times C \times 3$ by iterating NMDCS according to $IV$.

(3) It quantifies the chaotic sequence $Q$ using Eq. (15).

$$DQ = \text{floor}\left(Q \times 10^{15}\right) \tag{15}$$

(4) It computes the confusion key $SK_1 = \{SK_1(r, c, d)\}_{r\in\{1,\cdots,R\},c\in\{1,\cdots,C\},d\in\{1,2,3\}}$, where $SK_1(r, c, d)$ is computed using Eq. (16).

$$SK_1(r, c, d) = \text{mod}\left(DQ(r, c, d), 256\right) \tag{16}$$

(5) It computes the cross-plane key $SK_2 = \{SK_2(r, c, d)\}_{r\in\{1,\cdots,R\},c\in\{1,\cdots,C\},d\in\{1,2\}}$, where $SK_2(r, c, d)$ is computed using Eq. (17).

$$SK_2(r, c, d) = \text{mod}\left(DQ(r, c, d), D-d+1\right)+1 \tag{17}$$

### 3.1.2 Pixel confusion

Confusion is a nonlinear transformation that intricately disrupts the correlation between plain images and cipher images as well as between key and cipher images by changing pixels. In this section, the S-Box in [9] is used as the nonlinear confusion component to enhance the probabilistic statistical analysis resistance of our IEA-NMDCS algorithm, and the specific process is shown in Algorithm 2.

**Algorithm 1** Key derivation

```
Input: $MK$
Output: $SK_1, SK_2$
$IV \leftarrow$ Calculate the initial chaotic states using $MK$
$Q \leftarrow$ Iterate our NMDCS according to $IV$
$DQ \leftarrow$ Quantify $Q$ using Eq. (15)
$SK_1 \leftarrow$ Calculate the confusion key using $DQ$ and Eq. (16)
$SK_2 \leftarrow$ Calculate the cross-plane key using $DQ$ and Eq. (17)
Return $SK_1, SK_2$
```

**Algorithm 2** Pixel confusion

```
Input: $P, SK_1, R, C$
Output: Cipher image $E$
for $r = 1 : R$ do
    for $c = 1 : C$ do
        for $d = 1 : 3$ do
            $E(r, c, d) = \text{S-Box}(P(r, c, d) \oplus SK_1(r, c, d))$
        end for
    end for
end for
Return $E$
```

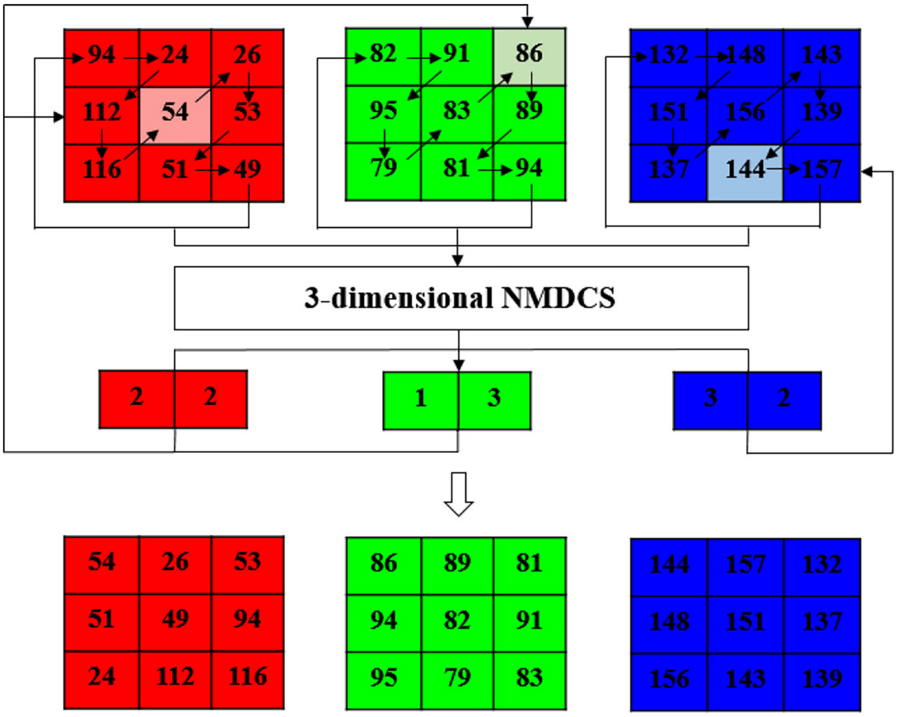
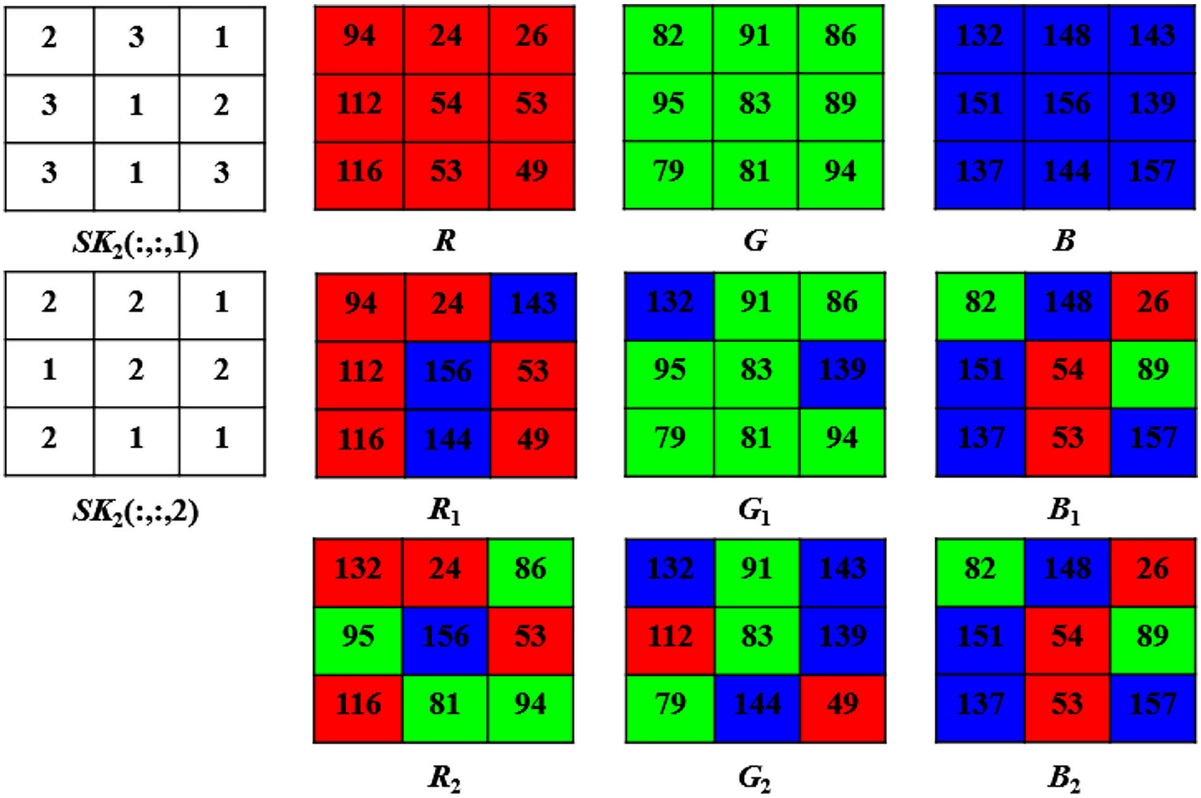


**Fig. 7** Schematic diagram of the adaptive zigzag transformation



| | | |
|---|---|---|
| 2 | 3 | 1 |
| 3 | 1 | 2 |
| 3 | 1 | 3 |

*SK*$_2$(:,:,1)

| | | |
|---|---|---|
| 🟥 94 | 🟥 24 | 🟥 26 |
| 🟥 112 | 🟥 54 | 🟥 53 |
| 🟥 116 | 🟥 53 | 🟥 49 |

*R*

| | | |
|---|---|---|
| 🟩 82 | 🟩 91 | 🟩 86 |
| 🟩 95 | 🟩 83 | 🟩 89 |
| 🟩 79 | 🟩 81 | 🟩 94 |

*G*

| | | |
|---|---|---|
| 🟦 132 | 🟦 148 | 🟦 143 |
| 🟦 151 | 🟦 156 | 🟦 139 |
| 🟦 137 | 🟦 144 | 🟦 157 |

*B*

| | | |
|---|---|---|
| 2 | 2 | 1 |
| 1 | 2 | 2 |
| 2 | 1 | 1 |

*SK*$_2$(:,:,2)

| | | |
|---|---|---|
| 🟥 94 | 🟥 24 | 🟦 143 |
| 🟥 112 | 🟦 156 | 🟥 53 |
| 🟥 116 | 🟦 144 | 🟥 49 |

*R*$_1$

| | | |
|---|---|---|
| 🟦 132 | 🟩 91 | 🟩 86 |
| 🟩 95 | 🟩 83 | 🟦 139 |
| 🟩 79 | 🟩 81 | 🟩 94 |

*G*$_1$

| | | |
|---|---|---|
| 🟩 82 | 🟦 148 | 🟥 26 |
| 🟦 151 | 🟥 54 | 🟩 89 |
| 🟦 137 | 🟥 53 | 🟦 157 |

*B*$_1$

| | | |
|---|---|---|
| 🟥 132 | 🟥 24 | 🟩 86 |
| 🟩 95 | 🟦 156 | 🟥 53 |
| 🟥 116 | 🟩 81 | 🟩 94 |

*R*$_2$

| | | |
|---|---|---|
| 🟦 132 | 🟩 91 | 🟦 143 |
| 🟥 112 | 🟩 83 | 🟦 139 |
| 🟩 79 | 🟦 144 | 🟥 49 |

*G*$_2$

| | | |
|---|---|---|
| 🟩 82 | 🟦 148 | 🟥 26 |
| 🟦 151 | 🟥 54 | 🟩 89 |
| 🟦 137 | 🟥 53 | 🟦 157 |

*B*$_2$

**Fig. 8** Schematic diagram of the cross-plane permutation

### *3.1.3 Adaptive zigzag transformation*

The correlation between neighboring pixels of a plain image can be effectively eliminated using the zigzag transformation. However, the initial position of the traditional zigzag transformation remains unaffected by the plain images, so minor alterations in a plain image will not transmit to the whole cipher image, resulting in its limited diffusion capability. To address the above problem, this section uses the mean value of the pixels and our NMDCS system to design a novel adaptive zigzag transformation that can improve the diffusion capability of our IEA-NMDCS algorithm while eliminating the correlation of neighboring pixels. The details are shown in Fig. 7.

(1) It calculates the average value of the pixels in each plane of the cipher image and records them as $\{e_d\}_{d\in\{1,2,3\}}$.

(2) It calculates the chaotic initial state $\boldsymbol{x}^0 = \{x_d^0\}_{d\in\{1,2,3\}}$ by Eq. (18).

$$x_d^0 = \frac{e_d}{128} - 1 \tag{18}$$

(3) It generates a chaotic sequence of length $T + 2$ using the NMDCS system, and records the last two chaotic states as $\boldsymbol{x}^{T+1} = \left\{x_d^{T+1}\right\}_{d\in\{1,2,3\}}$, and $\boldsymbol{x}^{T+2} = \left\{x_d^{T+2}\right\}_{d\in\{1,2,3\}}$.

(4) It calculates the initial coordinates of the rows and columns using Eqs. (19) and (20), and records them as $\boldsymbol{r}^0 = \{r_d^0\}_{d\in\{1,2,3\}}$ and $\boldsymbol{c}^0 = \{c_d^0\}_{d\in\{1,2,3\}}$ respectively.

$$r_d^0 = mod\left(floor\left(x_d^{T+1} \times 10^{15}\right), R\right) + 1 \tag{19}$$

$$c_d^0 = mod\left(floor\left(x_d^{T+2} \times 10^{15}\right), C\right) + 1 \tag{20}$$

(5) It performs a zigzag transformation on the cipher image starting at $\boldsymbol{r}^0 = \{r_d^0\}_{d\in\{1,2,3\}}$ and $\boldsymbol{c}^0 = \{c_d^0\}_{d\in\{1,2,3\}}$ respectively.

### 3.1.4 *Cross-plane permutation*

Due to color images consisting of three planes of red, green, and blue, the cross-plane permutation algorithm must be developed to remove the correlation of pixels across different planes. Our IEA-NMDCS algorithm uses the cross-plane permutation key and the shuffling algorithm to blur the pixels between different planes of the image. The specific process is shown in Fig. 8 and Algorithm 3.

**Algorithm 3** Cross-plane permutation

```
Input: $E$, $SK_2$, $R$, $C$
Output: Cipher image $E$
for $r = 1 : R$ do
    for $c = 1 : C$ do
        for $d = 1 : 2$ do
            $swap\left(E\left(r, c, 4-d\right), E\left(r, c, SK_2\left(r, c, d\right)\right)\right)$
        end for
    end for
end for
Return $E$
```

## 3.2 Security and efficiency analysis

This section evaluates the performance of our IEA-NMDCS algorithm from the following aspects. The test images are all taken from the USC-SIPI database and the CVG-UGR database.

### 3.2.1 *Key space analysis*

Key space is an important indicator reflecting the resistance of encryption algorithms to brute force attacks. The larger the key space, the more difficult it is to obtain the correct key through brute forces. Typically, a key space of at least $2^{100}$ possible secret keys is expected [36]. Since our IEA-NMDCS algorithm uses a 144-bit master key to generate derived subkeys, its key space is much larger than $2^{100}$. The above results show that our IEA-NMDCS algorithm is sufficient to withstand brute force attacks.

### 3.2.2 *NIST randomness test*

The National Institute of Standards and Technology (NIST) provides a series of guidelines for statistical tests known as the NIST Test Suite 800-22. In this section, the randomness of the cipher images obtained using the IEA-NMDCS algorithm has been evaluated through the application of this test suite. The test results are shown in Table 2.

**Table 2** NIST randomness test results

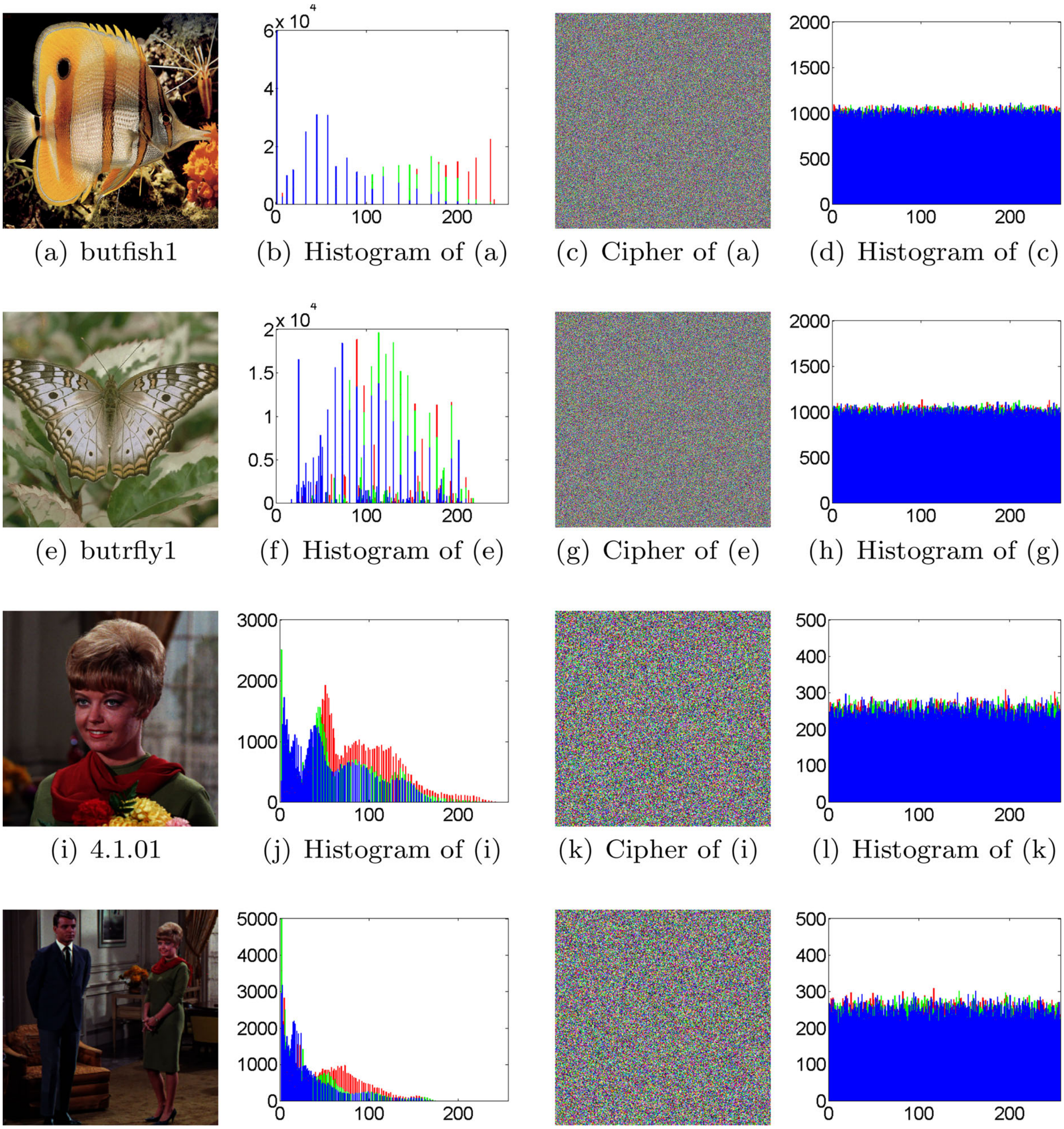
| Statistical test | *P*-value | Proportion | Result |
|---|---|---|---|
| Frequency | 0.616305 | 1 | Pass |
| Block frequency | 0.213309 | 0.98 | Pass |
| Cumulative sums 1 | 0.514124 | 1 | Pass |
| Cumulative sums 2 | 0.181557 | 1 | Pass |
| Runs | 0.366918 | 0.97 | Pass |
| Longest run | 0.867692 | 0.99 | Pass |
| Rank | 0.304126 | 0.98 | Pass |
| FFT | 0.851383 | 0.99 | Pass |
| Non overlapping template | 0.978072 | 1 | Pass |
| Overlapping template | 0.719747 | 0.98 | Pass |
| Universal | 0.657933 | 0.98 | Pass |
| Approximate entropy | 0.045675 | 1 | Pass |
| Random excursions | 0.585209 | 1 | Pass |
| Random excursions variant | 0.848588 | 1 | Pass |
| Serial 1 | 0.437274 | 0.98 | Pass |
| Serial 2 | 0.026948 | 0.98 | Pass |
| Linear complexity | 0.514124 | 0.99 | Pass |

It can be clearly seen from Table 2 that the P-value and proportions are all greater than 0.01 and 0.96 respectively. Therefore, the cipher images obtained using the IEA-NMDCS algorithm exhibit excellent randomness.

### 3.2.3 *Histogram analysis*

The histogram of an image can intuitively reflect the distribution of image pixels. In general, the histogram of a plaint image does not follow the uniform distribution, so it is susceptible to probabilistic statistical analysis. For an optimal encryption algorithm, the cipher images encrypted using the algorithm ought to conform to the uniform distribution. Figure 9 displays the histogram test results for the plain images and their cipher images encrypted with the IEA-NMDCS algorithm.

As can be seen from Fig. 9, the histogram of the plaint image exhibits an uneven distribution, whereas the histogram of its cipher image is uniformly dis-



(a) butfish1 (b) Histogram of (a) (c) Cipher of (a) (d) Histogram of (c)

(e) butrfly1 (f) Histogram of (e) (g) Cipher of (e) (h) Histogram of (g)

(i) 4.1.01 (j) Histogram of (i) (k) Cipher of (i) (l) Histogram of (k)

(m) 4.1.02 (n) Histogram of (m) (o) Cipher of (m) (p) Histogram of (o)

**Fig. 9** Histogram test results of the IEA-NMDCS algorithm

tributed, indicating that the cipher image does not leak any statistical information from the plain image.

To further demonstrate that the IEA-NMDCS algorithm can effectively withstand statistical analysis, we employ the chi-square test and the variance analysis to verify the uniformity of the histogram of the cipher images. The calculation methods for the chi-square test and the variance analysis are shown in Eq. (21) and [37], respectively.

$$\chi^2 = \sum_{i=1}^{256} \frac{(\eta_i - \mu)^2}{\mu} \tag{21}$$

**Table 3** Histogram analysis results

| Size | Name | $\chi^2$ value | Variance |
|---|---|---|---|
| 512 × 512 | Butfish1 | 278.3431 | 3340 |
| | Butrfly1 | 250.7715 | 3009 |
| | Cactusfl | 233.6686 | 2804 |
| | Clinmill | 227.7832 | 2733 |
| | Daisyfle | 245.4714 | 2946 |
| | Elephant | 276.9434 | 3323 |
| | Frog | 279.4447 | 3353 |
| | Goldgate | 243.4102 | 2921 |
| | Ivytree | 267.2324 | 3207 |
| | Malight | 253.0684 | 3037 |
| 256 × 256 | 4.1.01 | 251.7344 | 755 |
| | 4.1.02 | 248.6484 | 746 |
| | 4.1.03 | 254.3385 | 763 |
| | 4.1.04 | 281.1536 | 843 |
| | 4.1.05 | 267.9635 | 804 |
| | 4.1.06 | 242.5521 | 728 |
| | 4.1.07 | 290.8464 | 873 |
| | 4.1.08 | 246.8958 | 741 |

where $\eta_i$ and $\mu$ represent the number of observations and the expected number of each pixel in the image, respectively. We set a significance level $\alpha = 0.05$, and determine the following hypotheses using the chi-square test and the variance analysis. The analysis results are listed in Table 3.

$H_0$: The cipher images encrypted using the IEA-NMDCS algorithm are uniformly distributed.

$H_1$: The cipher images encrypted using the IEA-NMDCS algorithm are not uniformly distributed.

From Table 3, the Chi-square test values for the cipher images encrypted with the IEA-NMDCS algorithm are all less than $\chi^2_{0.05}(255) = 293.2478$. In addition, the histogram variance values of the $512 \times 512 \times 3$ and $256 \times 256 \times 3$ cipher images are approximately 3000 and 800, respectively. The above results indicate that the $H_0$ assumption is correct. In conclusion, the cipher images generated by the IEA-NMDCS algorithm are uniformly distributed, so they can effectively resist statistical analysis.

### *3.2.4 Key sensitivity analysis*

Key sensitivity refers to the fact that even minor alterations in the master key will produce an entirely different encryption or decryption result. A secure encryption algorithm must be sensitive to the master key. To test the key sensitivity of the IEA-NMDCS algorithm, we first randomly chose a master key $K_1$ = c1e**1**bda054ebc9f6accfd2f7c5ca9783618**2** of size 144-bit, and obtain the keys $K_2$ = c1e1bda054ebc9f6accfd2f7c5ca9783618**0** and $K_3$ = c1e**0**bda054ebc9f6accfd2f7c5ca97836182 by randomly changing 1-bit of $K_1$. Then,we encrypted and decrypted the images using $K_1$, $K_2$, and $K_3$ respectively. The specific results are shown in Figs. 10 and 11.

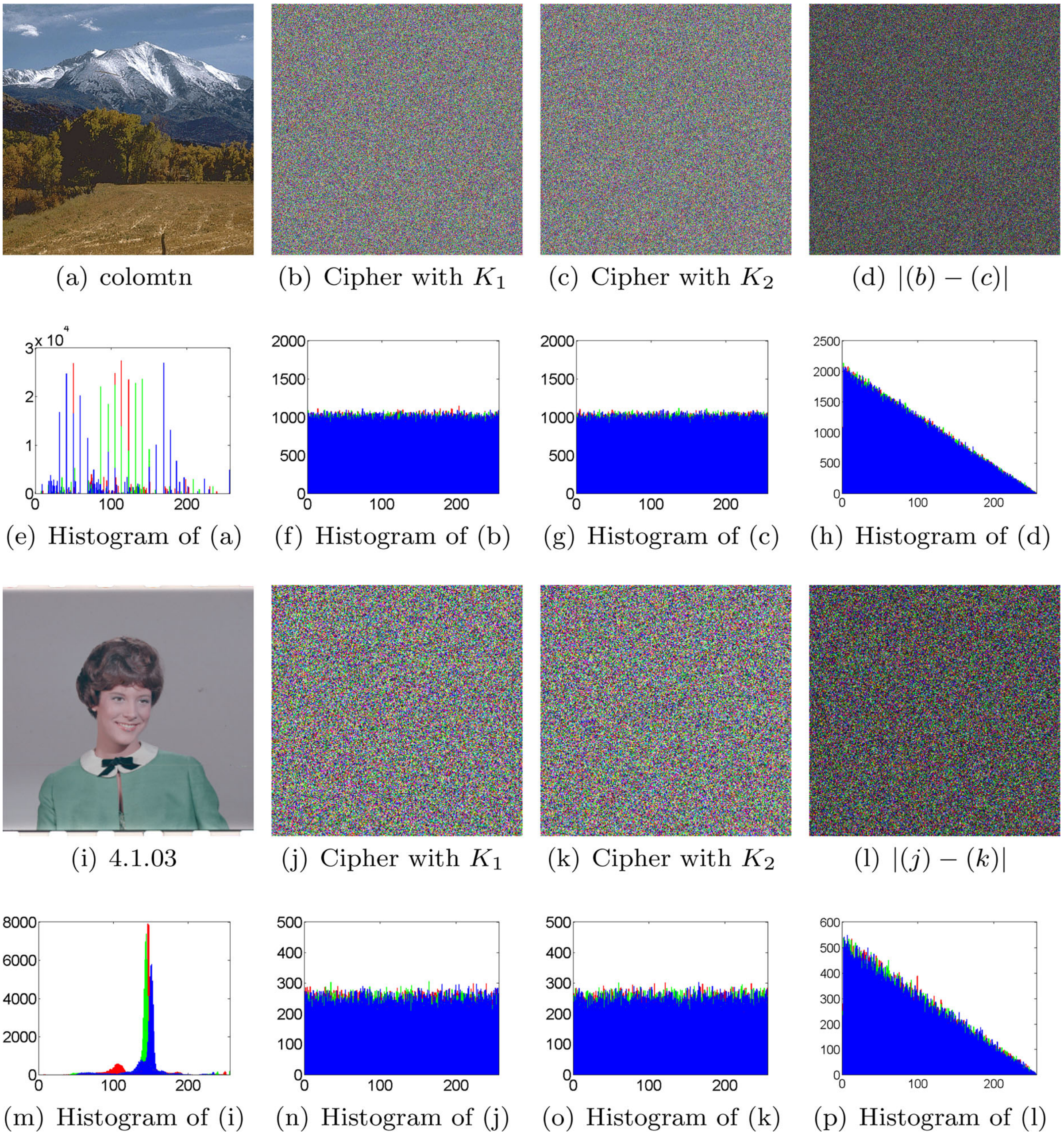
Figure 10 demonstrates that although the plain images have specific statistical features, the cipher images encrypted with the IEA-NMDCS algorithm are similar to the random noise, and they are completely different when using different keys. Therefore, our IEA-NMDCS algorithm is sensitive to the master key during the encryption process.

Figure 11 clearly illustrates that only decrypting the cipher image with the correct key will obtain the corresponding plain image, while the images decrypted by incorrect keys are similar to random noises. Furthermore, the images decrypted by different wrong keys are completely different. Therefore, our IEA-NMDCS algorithm is responsive to the master key utilized in the decryption procedure.

### *3.2.5 Sensitivity analysis for plain images*

Plaintext sensitivity refers to the capability of algorithms to withstand chosen plaintext attacks and differential attacks. Researchers commonly use the pixel change rate (NPCR) and normalized average change intensity (UACI) to assess the intensity of plaintext sensitivity. The calculation methods for these assessments are thoroughly described in [12]. The NPCR and UACI are anticipated to be 99.6094% and 33.4635% respectively. In addition, Wu et al. [38] have highlighted the necessity for NPCR values to surpass a defined threshold $N_\alpha$ and for UACI values to fall within the interval $\left(U_\alpha^-, U_\alpha^+\right)$, where $N_\alpha = 99.5693\%$ and $\left(U_\alpha^-, U_\alpha^+\right) = (33.2824\%, 33.6447\%)$ for an image of size $256 \times 256$, and $N_\alpha = 99.5893\%$ and $\left(U_\alpha^-, U_\alpha^+\right) = (33.3730\%, 33.5541\%)$ for an image of size $512 \times 512$. The NPCR and UACI scores for the cipher images encrypted using the IEA-NMDCS algorithm are displayed in Tables 4 and 5 respectively.

As is evidenced by Tables 4 and 5, the NPCR and UACI scores for the cipher images encrypted using



(a) colomtn (b) Cipher with $K_1$ (c) Cipher with $K_2$ (d) $|(b)-(c)|$

(e) Histogram of (a) (f) Histogram of (b) (g) Histogram of (c) (h) Histogram of (d)

(i) 4.1.03 (j) Cipher with $K_1$ (k) Cipher with $K_2$ (l) $|(j)-(k)|$

(m) Histogram of (i) (n) Histogram of (j) (o) Histogram of (k) (p) Histogram of (l)

**Fig. 10** Key sensitivity analysis during encryption

the IEA-NMDCS algorithm are all within the acceptable intervals, with values very close to 99.6094% and 33.4636% respectively. To further demonstrate the excellent plaintext sensitivity of our IEA-NMDCS algorithm, we use the 'Lena' as the plain image, and encrypt it using different image encryption algorithms. The NPCR and UACI comparison results can be found in Tables 6 and 7 respectively.

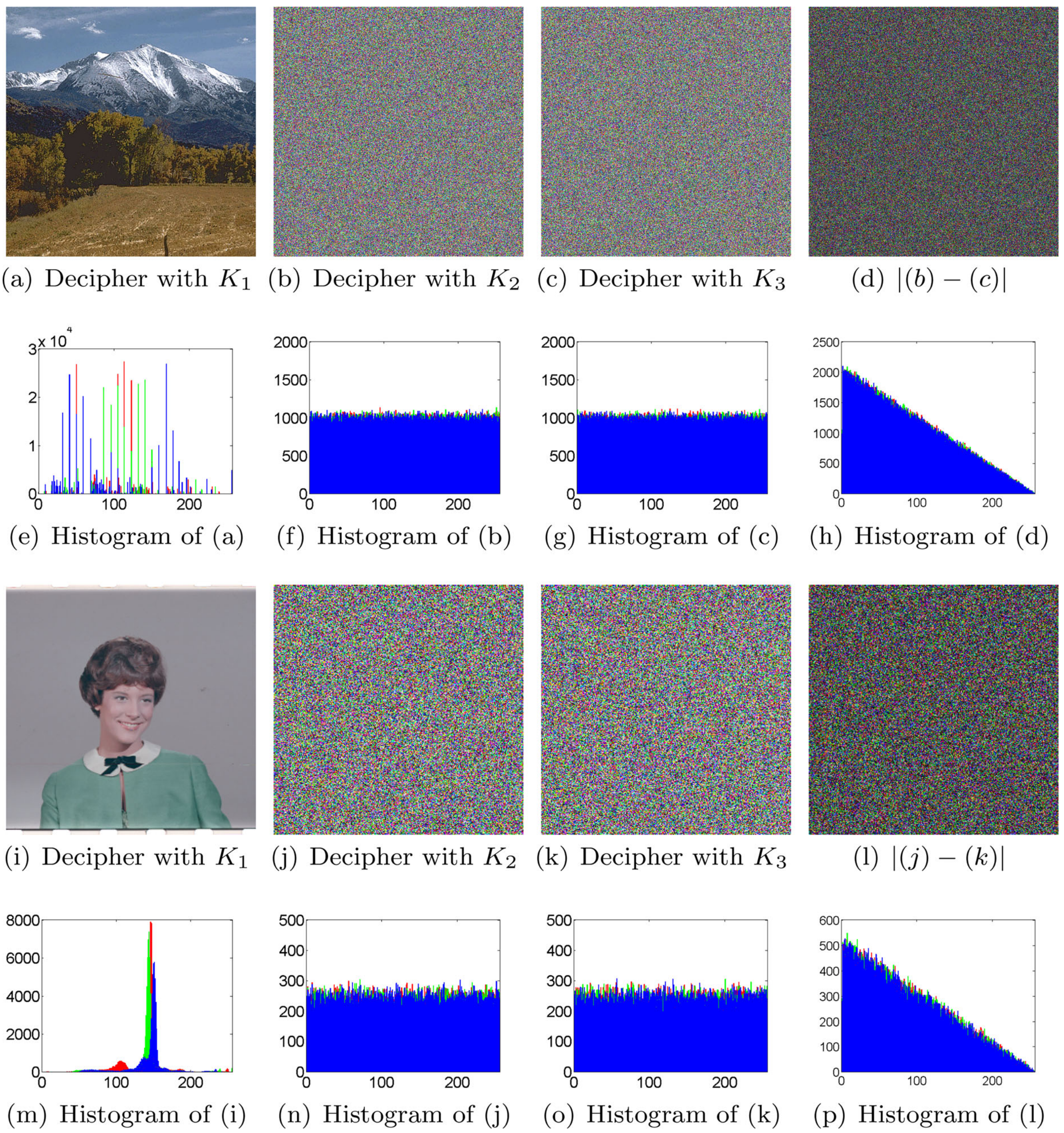
From Tables 6 and 7, the NPCR and UACI scores for the cipher images encrypted by different image algorithms are all within acceptable intervals, and the difference between them is very small, so they all

**Table 4** NPCR scores of cipher images

| Size | Name | NPCR (%) | | | Result |
|---|---|---|---|---|---|
| | | Red | Green | Blue | |
| 512 × 512 × 3 | Butfish1 | 99.6078 | 99.6151 | 99.6288 | Pass |
| | Butrfly1 | 99.6151 | 99.6124 | 99.6140 | Pass |
| | Cactusfl | 99.6006 | 99.6033 | 99.6170 | Pass |
| | Clinmill | 99.6136 | 99.6311 | 99.6078 | Pass |
| | Daisyfle | 99.6098 | 99.6140 | 99.6037 | Pass |
| | Elephant | 99.6437 | 99.6204 | 99.6040 | Pass |
| | Frog | 99.5991 | 99.5991 | 99.6101 | Pass |
| | Goldgate | 99.5983 | 99.6010 | 99.6140 | Pass |
| | Ivytree | 99.5960 | 99.6166 | 99.5930 | Pass |
| | Malight | 99.6235 | 99.6128 | 99.6170 | Pass |
| 256 × 256 × 3 | 4.1.01 | 99.6048 | 99.6475 | 99.6109 | Pass |
| | 4.1.02 | 99.6140 | 99.6155 | 99.6307 | Pass |
| | 4.1.03 | 99.6323 | 99.6262 | 99.6292 | Pass |
| | 4.1.04 | 99.6109 | 99.5911 | 99.5758 | Pass |
| | 4.1.05 | 99.6368 | 99.5850 | 99.5819 | Pass |
| | 4.1.06 | 99.6170 | 99.6124 | 99.6353 | Pass |
| | 4.1.07 | 99.6033 | 99.6002 | 99.6384 | Pass |
| | 4.1.08 | 99.6033 | 99.6078 | 99.6216 | Pass |

**Table 5** UACI scores of cipher images

| Size | Name | UACI (%) | | | Result |
|---|---|---|---|---|---|
| | | Red | Green | Blue | |
| 512 × 512 × 3 | Butfish1 | 33.4529 | 33.3967 | 33.4260 | Pass |
| | Butrfly1 | 33.3766 | 33.4334 | 33.5279 | Pass |
| | Cactusfl | 33.4937 | 33.5012 | 33.5210 | Pass |
| | Clinmill | 33.5413 | 33.4123 | 33.5003 | Pass |
| | Daisyfle | 33.4475 | 33.5117 | 33.4947 | Pass |
| | Elephant | 33.5385 | 33.4624 | 33.4987 | Pass |
| | Frog | 33.5020 | 33.4973 | 33.4018 | Pass |
| | Goldgate | 33.4002 | 33.4118 | 33.5402 | Pass |
| | Ivytree | 33.3869 | 33.5012 | 33.4981 | Pass |
| | Malight | 33.4213 | 33.4575 | 33.4257 | Pass |
| 256 × 256 × 3 | 4.1.01 | 33.3554 | 33.3785 | 33.3215 | Pass |
| | 4.1.02 | 33.3493 | 33.4199 | 33.4072 | Pass |
| | 4.1.03 | 33.4777 | 33.4334 | 33.5118 | Pass |
| | 4.1.04 | 33.3527 | 33.4463 | 33.4615 | Pass |
| | 4.1.05 | 33.5573 | 33.4068 | 33.5550 | Pass |
| | 4.1.06 | 33.4910 | 33.4287 | 33.5676 | Pass |
| | 4.1.07 | 33.4342 | 33.5995 | 33.5064 | Pass |
| | 4.1.08 | 33.6426 | 33.5013 | 33.5673 | Pass |



(a) Decipher with $K_1$ (b) Decipher with $K_2$ (c) Decipher with $K_3$ (d) $|(b) - (c)|$

(e) Histogram of (a) (f) Histogram of (b) (g) Histogram of (c) (h) Histogram of (d)

(i) Decipher with $K_1$ (j) Decipher with $K_2$ (k) Decipher with $K_3$ (l) $|(j) - (k)|$

(m) Histogram of (i) (n) Histogram of (j) (o) Histogram of (k) (p) Histogram of (l)

**Fig. 11** Key sensitivity analysis during decryption

achieve excellent plaintext sensitivity. However, the derived keys of the image encryption algorithms in [40,41] associated with plain images, and how to securely transmit the information has become a critical security bottleneck that constrains the application of such image encryption algorithms. Therefore, it can be deduced that our IEA-NMDCS algorithm is capable of withstanding chosen plaintext attacks and differential attacks.

### 3.2.6 Relevance analysis

Generally, the adjacent pixels in a plain image are highly correlated with each other. An excellent image

**Table 6** Comparison results of NPCR scores

| Algorithm | NPCR (%) | | | Result |
|---|---|---|---|---|
| | Red | Green | Blue | |
| Ours | 99.6239 | 99.6368 | 99.6071 | Pass |
| Hua [12] | 99.6479 | 99.6597 | 99.6288 | Pass |
| Wang [39] | 99.6016 | 99.6024 | 99.6089 | Pass |
| Gao [40] | 99.6153 | 99.6145 | 99.6147 | Pass |
| Hosny [41] | 99.6114 | 99.6095 | 99.6097 | Pass |
| Alawida [42] | 99.6243 | 99.6265 | 99.6109 | Pass |
| Zhou [43] | 99.6189 | 99.6132 | 99.6227 | Pass |
| Hua [44] | 99.6258 | 99.5991 | 99.6395 | Pass |

**Table 7** Comparison results of UACI scores

| Algorithm | UACI (%) | | | Result |
|---|---|---|---|---|
| | Red | Green | Blue | |
| Ours | 33.4842 | 33.5122 | 33.4762 | Pass |
| Hua [12] | 33.4390 | 33.4799 | 33.4833 | Pass |
| Wang [39] | 33.5041 | 33.4847 | 33.4423 | Pass |
| Gao [40] | 33.4631 | 33.4643 | 33.4689 | Pass |
| Hosny [41] | 33.4650 | 33.4812 | 33.4563 | Pass |
| Alawida [42] | 33.4734 | 33.5119 | 33.3821 | Pass |
| Zhou [43] | 33.3770 | 33.4473 | 33.4144 | Pass |
| Hua [44] | 33.5024 | 33.5405 | 33.4797 | Pass |

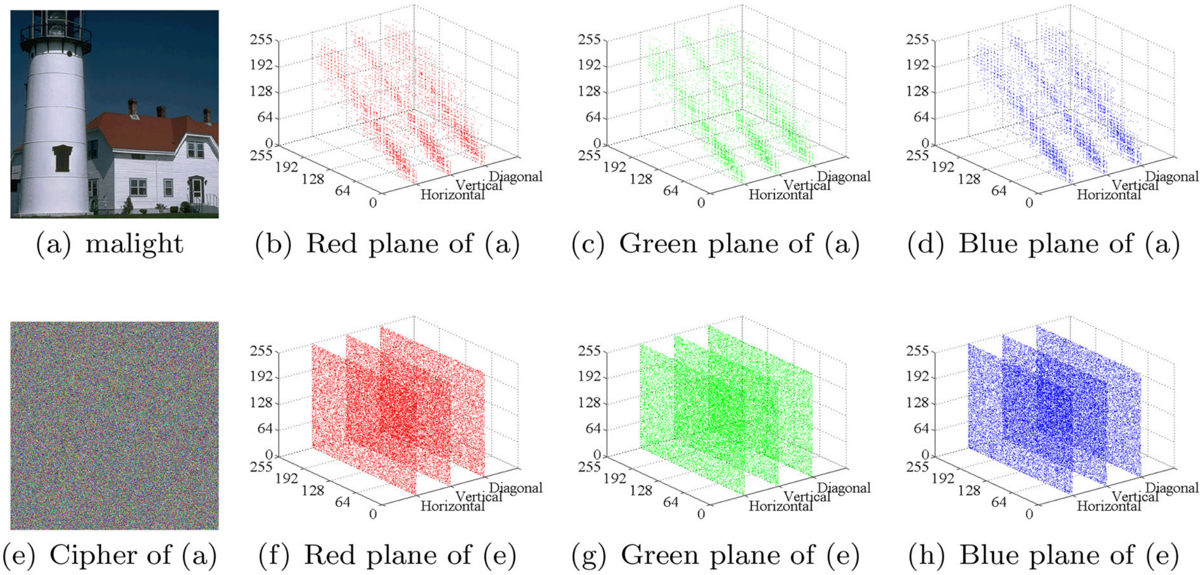
encryption algorithm should eliminate the correlation between adjacent pixels through substitution and permutation to enhance the pseudo-randomness of the cipher images. Consequently, the correlation between adjacent pixels becomes an essential indicator in the assessment of an algorithm's security. The correlation coefficient $R$ is calculated by Eq. (22).

$$\begin{cases} E(X) = \frac{\sum_{i=1}^{n} x_i}{n} \\ D(X) = \frac{\sum_{i=1}^{n} (x_i - E(X))^2}{n} \\ \operatorname{cov}(X, Y) = \frac{\sum_{i=1}^{n} (x_i - E(X))(Y_i - E(Y))}{n} \\ R(X, Y) = \frac{\operatorname{cov}(X,Y)}{\sqrt{D(X) \times D(Y)}} \end{cases} \tag{22}$$

where $X$ denotes the set consisting of image pixels, $Y$ denotes the set consisting of adjacent pixels of pixels in $X$, and $n$ is the number of pixels. The lower the correlation coefficient, the lower the correlation between adjacent pixels. In this section, we randomly select 12,000 pairs of adjacent pixels to calculate the correlation coefficients in the horizontal, vertical, and diagonal directions. The details are displayed in Fig. 12 and Table 8.

As can be seen from Fig. 12 and Table 8, it is clear that the adjacent pixels of the plain images exhibit a high level of correlation, whereas the adjacent pixels of their cipher images display very low correlation. In addition, the correlation between the adjacent pixels of the cipher images encrypted using the IEA-NMDCS algorithm is very close to the ideal value of 0. To further prove that our algorithm can withstand statistical attacks, we performed correlation coefficient comparison tests for different image encryption algorithms. The comparison results are shown in Table 9.

As illustrated in Table 9, the correlation coefficients of the cipher image encrypted with our IEA-NMDCS algorithm are closer to 0 than those of existing image encryption algorithms. The aforementioned results demonstrate that our image encryption algorithm is capable of effectively reducing the correlation among the adjacent pixels of images.



(a) malight (b) Red plane of (a) (c) Green plane of (a) (d) Blue plane of (a)

(e) Cipher of (a) (f) Red plane of (e) (g) Green plane of (e) (h) Blue plane of (e)

**Fig. 12** Diagram of correlation coefficients

**Table 8** Correlation coefficients of images

| Size | Name | Plain image | | | Cipher image | | |
|---|---|---|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| 512 × 512 | Butfish1 | 0.9472 | 0.9451 | 0.9209 | 0.0073 | 0.0075 | 0.0071 |
| | Butrfly1 | 0.9462 | 0.9532 | 0.9265 | 0.0076 | 0.0072 | 0.0074 |
| | Cactusfl | 0.8748 | 0.8743 | 0.8604 | 0.0072 | 0.0074 | 0.0075 |
| | Clinmill | 0.9382 | 0.9423 | 0.9095 | 0.0077 | 0.0076 | 0.0070 |
| | Daisyfle | 0.9772 | 0.9782 | 0.9621 | 0.0079 | 0.0073 | 0.0075 |
| | Elephant | 0.9835 | 0.9792 | 0.9706 | 0.0071 | 0.0072 | 0.0080 |
| | Frog | 0.9422 | 0.9537 | 0.9183 | 0.0070 | 0.0071 | 0.0069 |
| | Goldgate | 0.9526 | 0.9517 | 0.9290 | 0.0069 | 0.0075 | 0.0073 |
| | Ivytree | 0.8861 | 0.8795 | 0.8175 | 0.0069 | 0.0074 | 0.0073 |
| | Malight | 0.9770 | 0.9845 | 0.9675 | 0.0073 | 0.0078 | 0.0077 |
| 256 × 256 | 4.1.01 | 0.9564 | 0.9675 | 0.9464 | 0.0076 | 0.0082 | 0.0079 |
| | 4.1.02 | 0.9512 | 0.9328 | 0.9003 | 0.0070 | 0.0087 | 0.0080 |
| | 4.1.03 | 0.9183 | 0.9759 | 0.9015 | 0.0078 | 0.0078 | 0.0069 |
| | 4.1.04 | 0.9796 | 0.9655 | 0.9483 | 0.0082 | 0.0075 | 0.0087 |
| | 4.1.05 | 0.9514 | 0.9761 | 0.9367 | 0.0076 | 0.0080 | 0.0098 |
| | 4.1.06 | 0.9396 | 0.9631 | 0.9265 | 0.0076 | 0.0073 | 0.0078 |
| | 4.1.07 | 0.9824 | 0.9796 | 0.9641 | 0.0071 | 0.0077 | 0.0077 |
| | 4.1.08 | 0.9754 | 0.9732 | 0.9494 | 0.0079 | 0.0081 | 0.0069 |

**Table 9** Correlation coefficient comparison results

| Algorithm | Cipher image | | |
|---|---|---|---|
| | Red | Green | Blue |
| Ours | **0.0069** | **0.0073** | **0.0074** |
| Hua [12] | 0.0075 | 0.0074 | 0.0077 |
| Wang [39] | 0.0073 | 0.0074 | **0.0074** |
| Gao [40] | 0.0079 | 0.0075 | **0.0074** |
| Hosny [41] | 0.0078 | **0.0073** | 0.0077 |
| Alawida [42] | 0.0076 | **0.0073** | 0.0075 |
| Zhou [43] | 0.0081 | 0.0078 | 0.0081 |
| Hua [44] | 0.0073 | 0.0074 | 0.0080 |

Bold values indicate the optimal performance of the corresponding test items

**Table 10** Information entropy values of cipher images

| Size | Name | Plain image | | | Cipher image | | |
|---|---|---|---|---|---|---|---|
| | | Red | Green | Blue | Red | Green | Blue |
| 512 × 512 × 3 | Butfish1 | 4.1269 | 3.9930 | 3.7003 | 7.9993 | 7.9993 | 7.9994 |
| | Butrfly1 | 5.1634 | 5.0618 | 5.3168 | 7.9993 | 7.9993 | 7.9993 |
| | Cactusfl | 4.3969 | 4.2172 | 3.3881 | 7.9994 | 7.9993 | 7.9993 |
| | Clinmill | 5.6621 | 4.9586 | 5.2497 | 7.9993 | 7.9993 | 7.9994 |
| | Daisyfle | 4.1707 | 4.5775 | 3.0483 | 7.9993 | 7.9994 | 7.9994 |
| | Elephant | 4.8074 | 4.7543 | 4.3844 | 7.9993 | 7.9992 | 7.9994 |
| | Frog | 3.6277 | 4.9536 | 4.4948 | 7.9992 | 7.9993 | 7.9993 |
| | Goldgate | 3.8638 | 3.6124 | 4.2748 | 7.9992 | 7.9993 | 7.9993 |
| | Ivytree | 4.2258 | 4.7593 | 4.1692 | 7.9993 | 7.9992 | 7.9993 |
| | Malight | 4.9487 | 4.5272 | 4.6991 | 7.9994 | 7.9994 | 7.9992 |
| 256 × 256 × 3 | 4.1.01 | 6.4200 | 6.4457 | 6.3807 | 7.9972 | 7.9975 | 7.9973 |
| | 4.1.02 | 6.2499 | 5.9642 | 5.9309 | 7.9972 | 7.9975 | 7.9973 |
| | 4.1.03 | 5.7150 | 5.3738 | 5.7117 | 7.9971 | 7.9975 | 7.9972 |
| | 4.1.04 | 7.2549 | 7.2704 | 6.7825 | 7.9970 | 7.9974 | 7.9972 |
| | 4.1.05 | 6.4311 | 6.5389 | 6.2320 | 7.9974 | 7.9975 | 7.9968 |
| | 4.1.06 | 7.2104 | 7.4136 | 6.9207 | 7.9972 | 7.9969 | 7.9972 |
| | 4.1.07 | 5.2626 | 5.6947 | 6.5464 | 7.9972 | 7.9968 | 7.9970 |
| | 4.1.08 | 5.7920 | 6.2195 | 6.7986 | 7.9972 | 7.9977 | 7.9973 |

### *3.2.7 Information entropy*

In this section, we evaluate the pseudo-randomness of the cipher images using information entropy. Each pixel of an image contains 8 bits of information, so the theoretical maximum value of its information entropy is 8. Table 10 displays the information entropy values of the plain images and their cipher images encrypted using the IEA-NMDCS algorithm.

From Table 10, it can be seen that although the information entropy of the plain images is far less than the ideal value of 8, the information entropy of the cipher images encrypted with the IEA-NMDCS algorithm is very close to 8, indicating that the cipher images are uniformly distributed and have excellent pseudo-randomness. To further evaluate the encryption effect of the IEA-NMDCS algorithm, we encrypted the Lena image using the existing image encryption algorithms

**Table 11** Information entropy comparison results

| Algorithm | Cipher image | | |
|---|---|---|---|
| | Red | Green | Blue |
| Ours | 7.9993 | **7.9994** | **7.9994** |
| Hua [12] | **7.9994** | 7.9993 | **7.9994** |
| Wang [39] | 7.9993 | 7.9993 | 7.9993 |
| Gao [40] | 7.9993 | 7.9993 | 7.9993 |
| Hosny [41] | 7.9993 | **7.9994** | **7.9994** |
| Alawida [42] | 7.9992 | 7.9993 | 7.9993 |
| Zhou [43] | 7.9993 | 7.9993 | **7.9994** |
| Hua [44] | 7.9993 | 7.9993 | **7.9994** |

Bold values indicate the optimal performance of the corresponding test items

as well as our algorithm, and the information entropy values of the cipher images are listed in Table 11.

From Table 11, the information entropy values of the cipher image encrypted with our IEA-NMDCS algorithm are 7.9993, 7.9994, and 7.9994 respectively, which are better than those of existing image encryption algorithms except [12,41]. Thus, it can be concluded that our IEA-NMDCS algorithm can generate the cipher images with a uniform distribution that is highly resistant to probabilistic statistical analysis.

### *3.2.8 Efficiency analysis*

Efficiency is a crucial factor in evaluating the practicality of image encryption algorithms. Because decryption is the reverse process of encryption, it has the same algorithmic efficiency as encryption, this section only lists the comparison results of the encryption efficiency between the IEA-NMDCS algorithm and existing image encryption algorithms in Table 12.

From Table 12, it can be seen that the IEA-NMDCS algorithm is more efficient in encryption than the existing image encryption algorithms. This is mainly because our IEA-NMDCS algorithm does not require time-consuming numerical analysis methods to generate pseudo-chaotic sequences. Furthermore, it possesses efficient substitution and permutation operations.

**Table 12** Efficiency comparison results of image encryption algorithms

| Algorithm | Time-consuming (s) | |
|---|---|---|
| | 256 × 256 × 3 | 512 × 512 × 3 |
| Ours | **0.36** | **1.33** |
| Hua [12] | 1.72 | 6.52 |
| Wang [39] | 0.48 | 1.86 |
| Gao [40] | 1.29 | 4.92 |
| Hosny [41] | 2.67 | 9.12 |
| Alawida [42] | 1.86 | 7.45 |
| Zhou [43] | 1.70 | 18.98 |
| Hua [44] | 2.87 | 10.71 |

Bold values indicate the optimal performance of the corresponding test items

## 4 Conclusion

This paper first designs a non-degenerate multi-stable discrete chaotic system that can be demonstrated to exhibit the properties of multi-stability and non-degeneracy through rigorous theoretical analysis. Simulation experiments demonstrate that our discrete chaotic system exhibits strong chaotic behavior and high efficiency in terms of Lyapunov exponents, coexisting attractors, Poincaré sections, sensitivity to initial conditions, and iterative efficiency. Then, an efficient image encryption algorithm is proposed by combining the aforementioned discrete chaotic system and an adaptive zigzag transformation method. Simulation experiments show that our image encryption algorithm offers superior performance in terms of encryption and decryption efficiency, as well as impressive security properties, including histogram, key sensitivity, plaintext sensitivity, correlation between adjacent pixels, and information entropy. The proposed image encryption algorithm provides a robust foundation for the confidentiality protection of sensitive images in key industries, including government agencies, healthcare systems and financial institutions. In the future, we will design chaotic image compression and encryption algorithms based on the compressed perception theory, which can reduce the storage and transmission costs of sensitive images as well as ensure their confidentiality.

**Author contributions** Xiaojun Tong: Supervision, Writing review & editing, Funding Acquisition. Xudong Liu: Conceptualization, Methodology, Software, Writing original draft. Miao Zhang: Investigation. Zhu Wang: Validation. Yunhua Fan: Data curation.

**Funding** This work was supported by the following projects and foundations: Project ZR2019MF054 supported by Shandong Provincial Natural Science Foundation, National Natural Science Foundation of China (Grant No.61902091).

**Data availibility** The data that support the findings of this study are available from the corresponding author upon reasonable request.

**Declarations**

**Conflict of interest** The authors declare that they have no Conflict of interest.

## References

1. Hussain, S., Shah, T., Javeed, A.: Modified advanced encryption standard (MAES) based on non-associative inverse property loop. Multimed. Tools Appl. **82**(11), 16237–16256 (2023)
2. Liu, X., Tong, X., Wang, Z., Zhang, M., Fan, Y.: A novel devaney chaotic map with uniform trajectory for color image encryption. Appl. Math. Model. **120**, 153–174 (2023)
3. Liu, H., Kadir, A., Xu, C.: Cryptanalysis and constructing s-box based on chaotic map and backtracking. Appl. Math. Comput. **376**(1), 125153 (2020)
4. Jamal, S.S., Hazzazi, M.M., Khan, M.F., Bassfar, Z., Aljaedi, A., ul Islam, Z.: Region of interest-based medical image encryption technique based on chaotic s-boxes. Expert Syst. Appl. **238**, 122030 (2024)
5. Wang, X., Liu, C., Jiang, D.: A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. Expert Syst. Appl. **209**, 118426 (2022)
6. Ye, G., Du, S., Huang, X.: Image compression-hiding algorithm based on compressive sensing and integer wavelet transformation. Appl. Math. Model. **124**, 576–596 (2023)
7. Yang, F., Mou, J., Liu, J., Ma, C., Yan, H.: Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. Signal Process. **169**, 107373 (2020)
8. 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. **103**, 2867–2880 (2021)
9. Liu, X., Tong, X., Wang, Z., Zhang, M.: Uniform non-degeneracy discrete chaotic system and its application in image encryption. Nonlinear Dyn. **108**(1), 653–682 (2022)
10. Hua, Z., Zhou, B., Zhou, Y.: Sine-transform-based chaotic system with FPGA implementation. IEEE Trans. Industr. Electron. **65**(3), 2557–2566 (2017)
11. Choi, U.S., Cho, S.J., Kim, J.G., Kang, S.W., Kim, H.D.: Color image encryption based on programmable complemented maximum length cellular automata and generalized 3-D chaotic cat map. Multimed. Tools Appl. **79**, 22825–22842 (2020)
12. Hua, Z., Zhu, Z., Yi, S., Zhang, Z., Huang, H.: Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Info. Sci. **546**, 1063–1083 (2021)
13. Liu, X., Tong, X., Wang, Z., Zhang, M.: Efficient high nonlinearity s-box generating algorithm based on third-order nonlinear digital filter. Chaos, Solitons & Fractals **150**, 111109 (2021)
14. Hua, Z., Yi, S., Zhou, Y., Li, C., Wu, Y.: Designing hyperchaotic cat maps with any desired number of positive lyapunov exponents. IEEE Trans. Cybern. **48**(2), 463–473 (2017)
15. Wang, C., Fan, C., Ding, Q.: Constructing discrete chaotic systems with positive lyapunov exponents. Int. J. Bifurc. Chaos **28**(07), 1850084 (2018)
16. Zang, H., Liu, J., Li, J.: Construction of a class of high-dimensional discrete chaotic systems. Mathematics **9**(4), 365 (2021)
17. Liu, X., Tong, X., Zhang, M., Wang, Z., Fan, Y.: Image compression and encryption algorithm based on uniform non-degeneracy chaotic system and fractal coding. Nonlinear Dyn. **111**(9), 8771–8798 (2023)
18. Qin, M.: Yet new extreme multistable chaotic system. IEEE Trans. Circuits Syst. II: Expr. Br. **70**(8), 3124–3128 (2023)
19. Sriram, G., Ali, A.M.A., Natiq, H., Ahmadi, A., Rajagopal, K., Jafari, S.: Dynamics of a novel chaotic map. J. Comput. Appl. Math. **436**, 115453 (2024)
20. Ali, A.M.A., Sriram, S., Natiq, H., Ahmadi, A., Rajagopal, K., Jafari, S.: A novel multi-stable sinusoidal chaotic map with spectacular behaviors. Commun. Theor. Phys. **75**(11), 115001 (2023)
21. Huang, L., Li, C., Liu, J., Zhong, Y., Zhang, H.: A novel 3D non-degenerate hyperchaotic map with ultra-wide parameter range and coexisting attractors periodic switching. Nonlinear Dyn. **112**(3), 2289–2304 (2024)
22. Yang, L., Lai, Q.: Construction and implementation of discrete memristive hyperchaotic map with hidden attractors and self-excited attractors. Integration **94**, 102091 (2024)
23. 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 **152**, 111363 (2021)
24. Liu, X., Sun, K., Wang, H., He, S.: A class of novel discrete memristive chaotic map. Chaos, Solitons & Fractals **174**, 113791 (2023)
25. Di Marco, M., Forti, M., Pancioni, L., Tesi, A.: New class of discrete-time memristor circuits: First integrals, coexisting attractors and bifurcations without parameters. Int. J. Bifurc. Chaos **34**(01), 2450001 (2024)
26. Li, C., Luo, G., Qin, K., Li, C.: An image encryption scheme based on chaotic tent map. Nonlinear Dyn. **87**, 127–133 (2017)
27. Sang, Y., Sang, J., Alam, M.S.: Image encryption based on logistic chaotic systems and deep autoencoder. Pattern Recognit. Lett. **153**, 59–66 (2022)
28. Lai, Q., Lai, C., Zhang, H., Li, C.: Hidden coexisting hyperchaos of new memristive neuron model and its application in

image encryption. Chaos, Solitons & Fractals **158**, 112017 (2022)

29. Wang, S., Peng, Q., Du, B.: Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Optics Laser Technol. **148**, 107753 (2022)
30. Hua, Z., Jin, F., Xu, B., Huang, H.: 2D logistic-sine-coupling map for image encryption. Signal Process. **149**, 148–161 (2018)
31. Javeed, A., Shah, T., Ullah, A.: A color image privacy scheme established on nonlinear system of coupled differential equations. Multimed. Tools Appl. **79**(43), 32487–32501 (2020)
32. Wen, H., Liu, Z., Lai, H., Zhang, C., Liu, L., Yang, J., Lin, Y., Li, Y., Liao, Y., Ma, L., et al.: Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. Mathematics **10**(17), 3180 (2022)
33. Wang, M., Liu, H., Zhao, M.: Construction of a non-degeneracy 3D chaotic map and application to image encryption with keyed s-box. Multimed. Tools Appl. **82**(22), 34541–34563 (2023)
34. Ye, X., Wang, X.: Hidden oscillation and chaotic sea in a novel 3D chaotic system with exponential function. Nonlinear Dyn. **111**(16), 15477–15486 (2023)
35. Yang, Y., Huang, L., Kuznetsov, N.V., Lai, Q.: Design and implementation of grid-wing hidden chaotic attractors with only stable equilibria. IEEE Trans. Circuits Syst. I: Regul. Pap. **70**(12), 5408–5420 (2023)
36. Wu, Y., Zhang, L., Berretti, S., Wan, S.: Medical image encryption by content-aware DNA computing for secure healthcare. IEEE Trans. Industr. Info. **19**(2), 2089–2098 (2022)
37. Javeed, A., Shah, T., et al.: Lightweight secure image encryption scheme based on chaotic differential equation. Chin. J. Phys. **66**, 645–659 (2020)
38. Wu, Y., Noonan, J.P., Agaian, S., et al.: NPCR and UACI randomness tests for image encryption. Cyber J.: Multidiscipl. J. Sci. Technol. J. Selected Areas Telecommun. (JSAT) **1**(2), 31–38 (2011)
39. Wang, X., Gao, S.: Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a boolean network. Info. Sci. **539**, 195–214 (2020)
40. Gao, X., Sun, B., Cao, Y., Banerjee, S., Mou, J.: A color image encryption algorithm based on hyperchaotic map and DNA mutation. Chin. Phys. B **32**(3), 030501 (2023)
41. Hosny, K.M., Kamal, S.T., Darwish, M.M.: A novel color image encryption based on fractional shifted gegenbauer moments and 2D logistic-sine map. Vis. Comput. **39**(3), 1027–1044 (2023)
42. Alawida, M., Samsudin, A., Teh, J.S., Alkhawaldeh, R.S.: A new hybrid digital chaotic system with applications in image encryption. Signal Process. **160**, 45–58 (2019)
43. Zhou, Y., Hua, Z., Pun, C.M., Chen, C.P.: Cascade chaotic system with applications. IEEE Trans. Cybern. **45**(9), 2001–2012 (2014)
44. Hua, Z., Zhou, Y.: Design of image cipher using block-based scrambling and image filtering. Info. Sci. **396**, 97–113 (2017)

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.