Article

Not peer-reviewed version

Research on Wheat Image Encryption Based on Different Chaotic Systems

Yi Shao , Huiru Zhu , Xuefeng Deng , Hua Yang *

Posted Date: 18 January 2024

doi: 10.20944/preprints202401.1431.v1

Keywords: chaotic mapping; image encryption; wheat image

Article

Research on Wheat Image Encryption Based on Different Chaotic Systems

Yi Shao [1,2], Huiru Zhu [2], Xuefeng Deng [2] and Hua Yang [2,*]

[1] School of Software, Shanxi Agricultural University, Taigu 030801, China; s20222091@stu.sxau.edu.cn (Y. S.)
[2] College of Information Science and Engineering, Shanxi Agricultural University, Taigu 030801, China; s20222091@stu.sxau.edu.cn (Y. S.); z20223694@stu.sxau.edu.cn (H. Z.); dxf@sxau.edu.cn (X. D.); yanghua@sxau.edu.cn (H. Y.)
* Correspondence: yanghua@sxau.edu.cn

Abstract: (1) In order to study the influence of chaotic system on wheat image encryption, a method to find the optimal chaotic system encryption based on wheat image is proposed. (2) 10 different chaotic system schemes are combined to encrypt wheat images by 13 common chaotic maps, respectively. The best chaotic system scheme is obtained by considering the anti-attack capability of these encryption schemes, which analyzes 8 commonly used image encryption performance evaluation indexes. (3) The experimental results show that the new four-dimensional chaotic system has the best encryption effect, which is suitable for wheat image encryption. (4) The proposed scheme of wheat image encryption based on chaotic system provides a reference for other crop image encryption.

Keywords: chaotic mapping; image encryption; wheat image

1. Introduction

Wheat images contain data on wheat growth, pest monitoring and harvest prediction, which are important for agricultural researchers [1–5]. To protect the integrity, confidentiality and availability of sensitive data, wheat images should be encrypted. At the same time, in order to ensure the reliability and security of wheat production and research, it is necessary to prevent unauthorized access, tampering and leakage[6]. The image encryption technology based on chaos is used to protect wheat images. Chaotic image encryption is an encryption technology based on chaos theory, which uses chaotic system to generate pseudorandom number sequences to encrypt and decrypt images [7]. The chaotic system has the characteristics of high randomness, complexity and unpredictability [8], and are often used in image encryption. It can also provide higher anti-aggression and increase the difficulty of encrypted data being cracked. However, it is also necessary to select appropriate encryption schemes and parameters according to different needs to ensure the security and practicality of encryption algorithms.

In recent years, many scholars have made contributions to promoting the development of image encryption research. An image encryption scheme based on a new dynamic four-dimensional chaotic system, Z-type transformation and DNA operation is proposed by Zhao et al. [9], which has the characteristics of good security performance and resistance to various attacks. In order to realize the security and efficiency of the encryption algorithm, a color image encryption algorithm combining KAA mapping and multiple chaotic mappings is proposed by Alexan et al. [10]. Aiming at the problems of small key space and weak anti-differential attack capability of existing encryption algorithms, a chaotic image encryption scheme based on artificial fish swarm algorithm and DNA coding is proposed by Zhu et al. [11], which has better encryption performance and higher security. In order to solve the problem of too long computation time, composite crossover technology is introduced by Premkumar et al. [12], who proposed an image encryption technology based on genetic operators. In general, using chaotic system to encrypt images can effectively improve the security and confidentiality of image content. At the same time, it also has the advantages of high efficiency and flexibility, and has important application value in the field of image encryption.

 doi:10.20944/preprints202401.1431.v1

Chaotic image encryption is a widely used digital image encryption technology in recent years. According to different application fields, various color image encryption schemes are compared and analyzed by Ghadirli et al. [13], and their respective advantages and limitations are summarized. The characteristics, advantages and disadvantages of various chaotic systems used for image encryption are discussed by Suneja et al. [14]. By comparison, it is concluded that the security of image encryption based on low-dimensional chaotic system proposed earlier is low. So, in recent years, researchers have proposed various high-dimensional chaotic systems for image encryption. Due to the problem that traditional encryption algorithms cannot be used on resource-limited Internet of Things devices, a lightweight image encryption technology with losless, effective and anti-security attack capabilities is proposed by Roy et al. [15], which is based on two-dimensional von Neumann cellular automata. And the algorithm is suitable for implementation in real-time sensitive Internet of Things applications. A permisse-based private blockchain solution is proposed by Khan et al. [16], which stores the encrypted pixel value of the image on the blockchain, guaranteeing the privacy and security of the image data. Blockchain technology provides a solution for the encryption of sensitive image data for decentralized devices, which is suitable for the security needs of intelligent industries such as the Industrial Internet of Things. A symmetric key image encryption system based on piecewise linear chaotic mapping is proposed by Zhang et al. [17], which has the same encryption and decryption process, high encryption and decryption speed and the ability to resist plaintext attacks, and can be applied to actual communication. Combining sinusoidal mapping and fractional arithmetic, a new one-dimensional fractional chaotic mapping is proposed by Zhu et al. [18], which is used to design an image encryption algorithm based on parallel DNA coding. The experimental results show that the algorithm has good encryption performance and less time overhead, and has good application potential in secure communication applications. Different chaotic systems have different characteristics and are suitable for different image encryption tasks, which need to be selected according to specific needs.

In order to protect the security of agricultural information, it is necessary to build a scheme suitable for agricultural image encryption. An image-driven multi-feature plant management model based on feature data encryption scheme is constructed by Santhosh et al. [19], which used dynamic scheme and key to encrypt data, improving the security and performance of smart agriculture. Perumal et al. [20] realized data security of different smart devices in farmland by using data encryption schemes, which used different encryption schemes and keys to encrypt data of farmland devices controlled by users, thus achieving higher accuracy of low-rate attack detection. A new homomorphic encryption algorithm is proposed by Kulalvaimozhi et al. [21], which combined with the compression process to encrypt field crop images, reducing the encryption time and preserving high-quality reconstructed images. A method combining Logistic-Sine and Logistic-Tent chaotic system is proposed by Padmapriya et al. [22] to encrypt agricultural image information, which is effective and robust.

After analyzing the above literature, it is found that a good image encryption scheme is very important for the development of smart agriculture. However, there are too few agricultural image encryption algorithms based on chaotic systems, so it is impossible to know whether the performance of different chaotic systems in agricultural image encryption is good or bad. In order to solve the problem of wheat image encryption, in this paper, the existing popular chaotic system is applied to wheat image encryption algorithm, and compares and analyzes the common image encryption performance evaluation index to measure its encryption effect. The aim is to find the most suitable chaotic system scheme for wheat image encryption, and provide a reference for agricultural image encryption scheme based on chaotic system.

The 10 chaotic system schemes proposed in this paper include Piecewise Linear Chaotic Map (PWLCM) chaotic mapping, Sine mapping, Tent mapping, Logistic mapping, Lorenz system, Rossler system, Chen system, hyper-chaotic Chen system, hyper-chaotic Lorenz system, hyper-chaotic Rossler system, hyper-chaotic Hide-Skeldon-Acheson system, new four-dimensional chaotic system, hyper-chaotic Lü system.

The main contributions of this paper are as follows:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

1.The image encryption algorithm based on chaotic system is applied to wheat image encryption. 2. An encryption scheme for selecting a suitable chaotic system based on wheat images is proposed. 3. By comparing 8 common evaluation indexes of image encryption performance, the new four-dimensional chaotic system is selected as the most suitable for wheat image encryption.

2. Chaotic Systems

Chaotic system is a mathematical model describing chaotic dynamic system, which is characterized by high nonlinearity, complexity and unpredictability [23]. The output sequence of chaotic systems is pseudo-random and highly sensitive to initial conditions [24], which makes chaotic systems have a wide range of applications in the fields of encryption and pseudo-random number generation. In digital image encryption system, chaotic system is mainly used to generate chaotic sequence [25], which is used to generate encryption key, pixel replacement, initialize encryption algorithm and other operations.

Common one-dimensional chaotic systems are as follows:

1. Sine map:

$$x_{t+1}=S(x)=\varepsilon\sin(\pi x_t) \tag{1}$$

where $\varepsilon \in [0,1]$ is the control parameter, $x_t \in [0,1]$ is the status value of the system at time t.

2. Tent map:

$$x_{t+1}=T(x)=\begin{cases}2\varepsilon x_t, & x_t<0.5\\ 2\varepsilon(1-x_t), & x_t\geq 0.5\end{cases} \tag{2}$$

3. Logistic map:

$$x_{t+1}=L(x)=4\varepsilon x_t(1-x_t) \tag{3}$$

4. PWLCM map:

$$x_{t+1}=\begin{cases}\frac{x_t}{\varepsilon}, & x_t\in[0,\varepsilon)\\ \frac{1-x_t}{1-\varepsilon}, & x_t\in(\varepsilon,1]\end{cases} \tag{4}$$

Common high-dimensional chaotic systems are as follows:

5. Chen system:

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=(c-a)x-xz+cy\\ \dot{z}=xy-bz\end{cases} \tag{5}$$

where $a=35$, $b=3$, and $c\in[20, 28.4]$. The x, y, and z are the status values of the system at time t. The $\dot{x}$, $\dot{y}$, and $\dot{z}$ represent the derivative of the independent variable x, y, and z at time t.

6. hyper-chaotic Chen system:

$$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=-xz+dx+cy-w\\ \dot{z}=xy-bz\\ \dot{w}=x+k\end{cases} \tag{6}$$

where $a=36$, $b=3$, $c=28$, $d=-16$, and $-0.7\leq k\leq 0.7$. The w is the status value of the system at time t. The $\dot{w}$ represents the derivative of the independent variable w at time t.

7. Lorenz system:

$$\begin{cases}\dot{x}=-a(x-y)\\ \dot{y}=-xz+bx-y\\ \dot{z}=xy-cz\end{cases} \tag{7}$$

where $a=10$, $b=28$, and $c=8/3$.

8. hyper-chaotic Lorenz system:

 doi:10.20944/preprints202401.1431.v1

$$\begin{cases} \dot{x}=a(y-x)+w \\ \dot{y}=cx-y-xz \\ \dot{z}=xy-bz \\ \dot{w}=-yz+kw \end{cases} \quad (8)$$

where a=10, b=8/3, c=28, d=-16, and -1.52≤k≤-0.06.

9. Rossler system:

$$\begin{cases} \dot{x}=-ay-z \\ \dot{y}=ax+by \\ \dot{z}=c+z(x-d) \end{cases} \quad (9)$$

where a=1.0, b=0.165, c=0.2, and d=10.

10. hyper-chaotic Rossler system:

$$\begin{cases} \dot{x}=-y-z \\ \dot{y}=x+ax+w \\ \dot{z}=b+xz \\ \dot{w}=-cz+dw \end{cases} \quad (10)$$

where a=0.25, b=3, c=0.5, and d=0.05.

11. hyper-chaotic Hide-Skeldon-Acheson system [26]:

$$\begin{cases} \dot{x}=-y-z \\ \dot{y}=x+ax+w \\ \dot{z}=b+xz \\ \dot{w}=-cz+dw \end{cases} \quad (11)$$

where a=0.01, b=30, c=0, d=2, e=0.001, f=28.5, g=1, k=1.2, q=0, and h=0.

12. New four-dimensional chaotic system [27]:

$$\begin{cases} \dot{x}=-y-z \\ \dot{y}=x+ax+w \\ \dot{z}=b+xz \\ \dot{w}=-cz+dw \end{cases} \quad (12)$$

where a=25, b=3, c=18, d=19, and e=14.

13. hyper-chaotic Lü system [28]:

$$\begin{cases} \dot{x}=y-ax \\ \dot{y}=bz-xz \\ \dot{z}=xy-xw \\ \dot{w}=-x+c \end{cases} \quad (13)$$

where a=10, b=3, and c=12.

3. Algorithm Description

3.1. Original Image Encryption Algorithm

An algorithm to modify the initial conditions and control parameters of PWLCM, Lorenz and hyper-chaotic Chen systems by using SHA-256 hash function is proposed by ur Rehman[29] and selected for color image encryption. The scheme consists of four stages: two scrambling operations, DNA encoding and DNA decoding. In the first scrambling process, the red, green and blue channels of the original color image are arranged into one-dimensional vectors, and the chaotic sequence obtained by PWLCM is used to reorder them. Then, the sorted pixel list is re-divided into red, green, and blue channels. In the second scrambling process, Lorenz system is used to generate three chaotic sequences, and the red, green and blue channels obtained after the first scrambling are rearranged respectively. After two scrambling operations, hyper-chaotic Chen system is used to generate four chaotic sequences, namely U, V, W and X. The sequence U is divided into three subvectors, which select DNA coding rules according to Table 1. The value of each pixel in the red, green and blue channels is converted to the DNA base. In the pixel-level confusion stage, the XOR rules based on

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

DNA bases are shown in Table 2. Xor operations are performed on the red, green, and blue channels above using the DNA replacement rules shown in Table 3. In addition, the sequence V is used to select DNA rules, and the sequence W is used to determine the number of repeated iterations of the XOR operation. The sequence X is then divided into three subvectors, which select the DNA decoding rules according to Table 1. Realize the conversion of DNA bases to values for each pixel in the red, green and blue channels. Finally, the three decoded red, green and blue channels are combined to get the encrypted image.

Table 1. Encoding and decoding rules of DNA.

Rule	Chaotic intervals	Encoding	Decoding
1	0.01-0.05, 0.20-0.25, 0.40-0.45, 0.50-0.55, 0.95-0.99	AGCT	GTAC
2	0.05-0.10, 0.30-0.35, 0.60-0.65, 0.70-0.75, 0.85-0.90	ACGT	TGCA
3	0.10-0.15, 0.35-0.40, 0.55-0.60, 0.65-0.70, 0.80-0.85	GATC	CTAG
4	0.15-0.20, 0.25-0.30, 0.45-0.50, 0.75-0.80, 0.90-0.95	CATG	TCGA

Table 2. XOR operations for DNA Bases.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Table 3. DNA rules for Substitution.

Value	0	1	2	3	4	5	6	7
DNA Rules for XOR	AGCT	GATC	CTAG	TGCA	GTAC	ACGT	TCGA	CATG

3.2. Image Encryption Schemes Based on Different Chaotic Systems

Based on Section 3.1, it can be seen that three chaotic systems, PWLCM, Lorenz and Chen, are used in the color image encryption algorithm proposed by ur Rehman [29]. In order to compare the effect of different chaotic systems on wheat image encryption, we apply this algorithm to wheat image encryption. And the above three chaotic systems are replaced successively to find the most suitable chaotic system scheme for wheat image encryption.

Based on the original image encryption scheme, the specific replacement scheme is as follows:

Scheme 1: Replace the PWLCM with the Sine mapping.

Scheme 2: Replace the PWLCM with the Tent mapping.

Scheme 3: Replace the PWLCM with the Logistic mapping.

Scheme 4: Replace the Lorenz system with the Rossler system.

Scheme 5: Replace the Lorenz system with the Chen system.

Scheme 6: Replace the hyper-chaotic Chen system with the hyper-chaotic Lorenz system.

Scheme 7: Replace the hyper-chaotic Chen system with the hyper-chaotic Rossler system.

Scheme 8: Replace the hyper-chaotic Chen system with the hyper-chaotic Hide-Skeldon-Acheson system.

Scheme 9: Replace the hyper-chaotic Chen system with the new four-dimensional chaotic system.

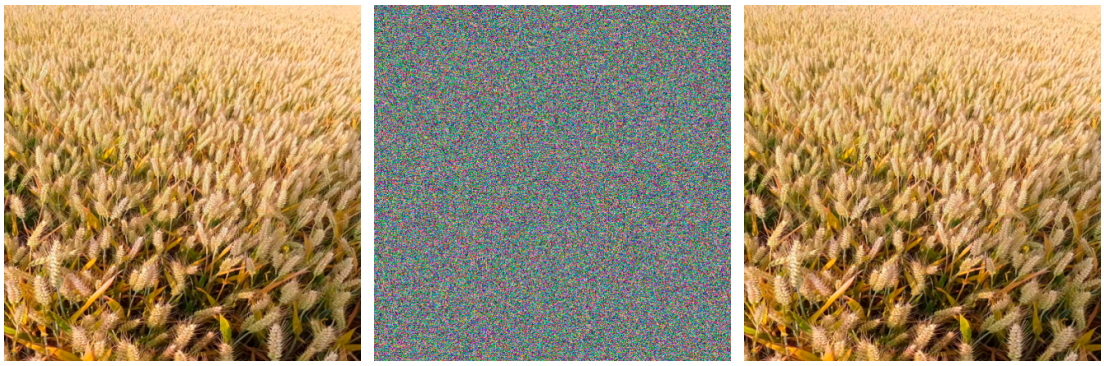
Scheme 10: Replace the hyper-chaotic Chen system with hyper-chaotic Lü system.

4. Results and Discussion

The experimental platform is a PC with an 13th Gen Intel(R) Core(TM) i5-13400F @ 2.50 GHz CPU, 32.0 GB memory, NVIDIA GeForce RTX 4060 graphics, and Windows 11 operating system.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

Based on the encryption scheme mentioned in section 3, taking the wheat image of Gaoping City, Shanxi Province as an example, the encryption and decryption of the wheat encryption system is shown in Figure 1.



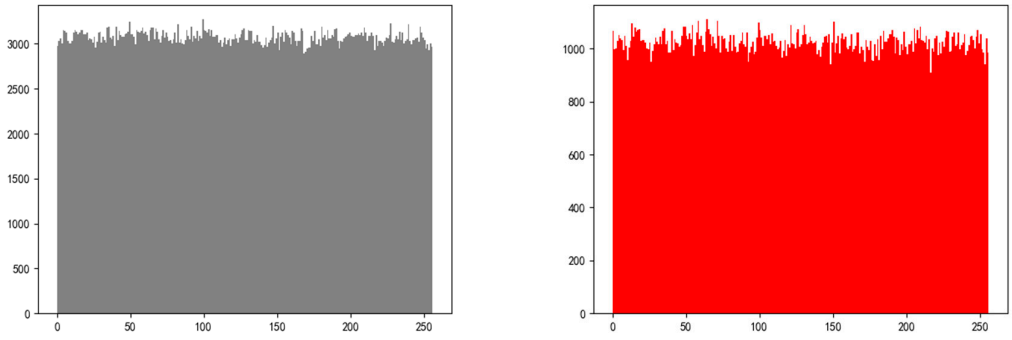
(**a**) (**b**) (**c**)

Figure 1. Image of wheat encryption and decryption process. (**a**) The original image; (**b**) The encrypted image; (**c**) The decrypted image.

4.1. Histogram Analysis

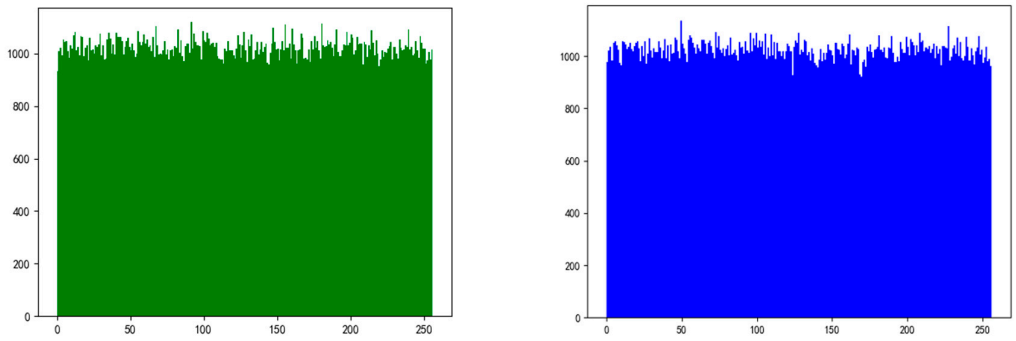
Histogram refers to the graph drawn by the frequency of each gray value in the statistical image, reflecting the most basic statistical characteristics of the image [30]. In order to resist statistical analysis attacks, the histogram of the encrypted image should be as evenly distributed as possible. Variance is used to measure the frequency distribution of the histogram, and the calculation formula is shown in equation (16). The smaller the variance, the more uniform the pixel distribution. The arithmetic square root of the variance is called the standard deviation, which reflects the degree of dispersion in a data set.

The histogram of wheat encryption image of Gaoping City based on scheme 1 is shown in Figure 2. Table 4 compares the values of variance and standard deviation in each scheme. The results show that the variance and standard deviation of scheme 7 are the best, while the variance and standard deviation of scheme 9 are the worst.



(**a**) (**b**)

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1



(**c**) (**d**)

Figure 2. The histogram of the encrypted image. (**a**) Encrypted image; (**b**) Channel R; (**c**) Channel G; (**d**) Channel B.

Table 4. Variance and standard deviation of wheat encrypted images.

Chaotic System Scheme	1	2	3	4	5	6	7	8	9	10
Variance	5458.30	5453.56	5446.62	5450.37	5459.35	5448.77	5443.85	5446.41	6356.91	5897.04
Standard Deviation	73.88	73.85	73.80	73.83	73.89	73.82	73.78	73.80	79.73	76.79

4.2. Correlation Analysis of Adjacent Pixels

The correlation of adjacent pixels refers to the correlation degree of pixel values in adjacent positions of an image [31], and the calculation formula is as follows:

$$R_{uv} = \frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{14}$$

$$\mathrm{cov}(u,v) = \frac{1}{N}\sum_{n=1}^{N}(u_n - E(u))(v_n - E(v)) \tag{15}$$

$$D(u) = \frac{1}{N}\sum_{n=1}^{N}(u_n - E(u))^2 \tag{16}$$

$$E(u) = \frac{1}{N}\sum_{n=1}^{N}u_n \tag{17}$$

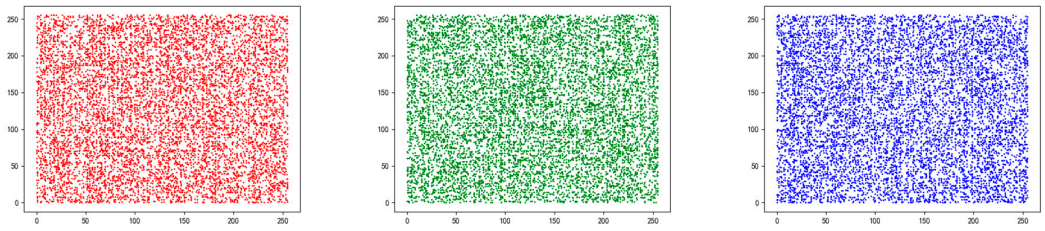
where v is the adjacent pixel of u, and $\mathrm{cov}(u,v)$ is the covariance at two pixels u and v, respectively. The N is the total number of pixels in the image. $E(u)$ is the mean, $D(u)$ is the variance, and $\sqrt{D(u)}$ is the standard deviation, respectively. The R_{uv} is the correlation of adjacent pixels.

Generally speaking, there is a strong correlation between adjacent pixels in the horizontal, vertical and diagonal directions in a plaintext image. This feature is often used by attackers to infer the values of adjacent pixels from the values of known pixels, thus cracking encrypted images. A good image encryption algorithm should be able to reduce the correlation between adjacent pixels and achieve zero correlation as far as possible.

The correlation of adjacent pixels of wheat encryption image of Gaoping City based on scheme 1 is shown in Figure 3. Tables 5–7 lists the values of each scheme for the correlation of adjacent pixels

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

in the horizontal, vertical, and diagonal directions. In general, scheme 9 shows good correlation, with the value most close to 0. Moreover, it is found that the correlation on the R, G and B channels of the same scheme will also show great differences. So, the difference in the color of the original image will also affect the choice of the best scheme.



(**a**) (**b**) (**c**)

Figure 3. The correlation of encrypted image. (**a**) Channel R; (**b**) Channel G; (**c**) Channel B.

Table 5. Horizontal correlation of wheat encrypted images.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
Correlation	R	0.0080	0.0018	-0.0251	0.0315	-0.0329	0.0050	-0.0202	-0.0186	-0.0000	0.0276
	G	-0.0309	-0.0137	0.0117	-0.0149	0.0173	-0.0126	0.0093	0.0068	-0.0019	0.0166
	B	-0.0194	-0.0081	-0.0281	0.0243	0.0230	-0.0023	0.0318	0.0399	0.0111	0.0095

Table 6. Vertical correlation of wheat encrypted images.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
Correlation	R	0.0113	0.0095	-0.0029	0.0037	0.0178	0.0177	0.0127	-0.0094	0.0159	0.0114
	G	0.0158	0.0153	0.0499	0.0079	0.0082	0.0284	0.0087	-0.0098	-0.0121	-0.0066
	B	0.0351	0.0372	0.0168	0.0244	0.0350	-0.0189	0.0036	0.0032	0.0223	0.0093

Table 7. Diagonal correlation of wheat encrypted images.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
Correlation	R	0.0319	0.0145	-0.0087	0.0293	-0.0105	-0.0023	-0.0130	-0.0057	0.0018	-0.0208
	G	0.0160	0.0004	0.0021	0.0123	-0.0073	0.0054	-0.0203	0.0230	-0.0156	-0.0363
	B	-0.0004	0.0154	-0.0265	0.0097	-0.0234	-0.0026	0.0263	0.0265	-0.0003	-0.0099

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

4.3. Key Sensitivity Analysis

Key sensitivity analysis aims to analyze the difference between two ciphertext images obtained from the same plaintext image that is encrypted when the key changes slightly [32]. If two ciphertext images are significantly different, it is said that the key sensitivity of the image cryptosystem is strong. If the difference between two ciphertext images is small, the key sensitivity is poor. A good image encryption system should have strong key sensitivity. The Normalized Pixel Contrast Ratio (NPCR) and Unified Average Changing Intensity (UACI) are commonly used to measure the difference between two images of the same size. NPCR is used to compare the values of pixels in the corresponding positions of two images, and record the proportion of the number of different pixels in all pixels. The calculation formula is as follows:

$$\mathrm{NPCR}(Q_1, Q_2) = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}\left|\mathrm{Sign}(Q_1(i,j) - Q_2(i,j))\right| \times 100\% \tag{18}$$

$\mathrm{Sign}(\cdot)$ is a symbolic function, defined as follows:

$$\mathrm{Sign}(\tau) = \begin{cases} 1, & \tau > 0 \\ 0, & \tau = 0 \\ -1, & \tau < 0 \end{cases} \tag{19}$$

where W and H are the width and height of the image, respectively. $Q_1(i,j)$ and $Q_2(i,j)$ are the pixel values at the position of the first image and the second image, respectively.

UACI is used to first record the difference of pixels in the corresponding positions of the two images. Then calculate the average value of the ratio between the difference and the maximum difference (that is, 255) of all pixels at the corresponding position. The calculation formula is as follows:

$$\mathrm{UACI}(Q_1, Q_2) = \frac{1}{WH}\sum_{i}^{W}\sum_{j}^{H}\frac{\left|Q_1(i,j) - Q_2(i,j)\right|}{255 - 0} \times 100\% \tag{20}$$

Due to the randomness of the location, the theoretical expected values of NPCR and UACI for the two random images are 99.6094% and 33.4635%, respectively.

The NPCR and UACI values of wheat encryption images in Gaoping City in each scheme are shown in Table 8. In general, the NPCR value of scheme 1 is closest to the theoretical expected value of 99.6094%, and the UACI value of scheme 9 is closest to the theoretical expected value of 33.4635%. In addition, the NPCR and UACI values of different R, G and B channels may have great differences.

Table 8. NPCR and UACI values of wheat encrypted images.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
NPCR (%)	R	99.6056	99.6231	99.6059	99.6059	99.6078	99.5899	99.6040	99.6113	99.6223	99.6098
	G	99.6094	99.6243	99.5979	99.6193	99.6208	99.6349	99.6189	99.6017	99.6269	99.6204
	B	99.6094	99.6078	99.6113	99.6082	99.6223	99.5975	99.6124	99.6113	99.6368	99.6353
UACI (%)	R	31.4796	31.6308	31.3929	31.3833	31.1587	31.4013	31.4481	31.4044	33.0811	32.1839
	G	31.4107	31.5910	31.4502	31.4147	29.5023	31.4897	31.3795	31.4747	33.0621	32.1632
	B	31.3855	31.5985	31.4365	31.4664	33.2818	31.4660	31.3408	31.4391	33.1365	32.2219

4.4. Key Space Analysis

Key space refers to the set of all legal keys [33]. The key space of an image encryption system should be large enough to effectively combat exhaustive attacks. According to the current computer level, the key space of the encryption algorithm should generally be greater than 2^{128}. The key spaces

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

of each scheme are shown in Table 9. The key space of scheme 6 and scheme 10 is the smallest, which is $10^{84} \cong 2^{280} > 2^{128}$. The key space of scheme 8 is the largest, which is 10^{154}. And the key space of scheme 4 and scheme 9 is the second largest , which is 10^{104}.

Table 9. Key space.

Chaotic System Scheme	1	2	3	4	5	6	7	8	9	10
Key Space	10^{94}	10^{94}	10^{94}	10^{104}	10^{94}	10^{84}	10^{94}	10^{154}	10^{104}	10^{84}

4.5. Information Entropy

Information entropy is used to measure the uniformity of gray value distribution in images, reflecting the uncertainty of image information [34]. Generally speaking, the greater the information entropy of an image, the greater the uncertainty. Then, the more uniform the distribution of gray values of pixels, the less visible information, and the stronger the resistance to entropy attacks. The calculation formula of information entropy is as follows:

$$I = -\sum_{m=0}^{L} p(m)\log_2 p(m) \tag{21}$$

where L is the number of gray levels of the image. $p(m)$ is the probability that the gray value m occurs. For a gray random image with $L = 256$, the theoretical value of information entropy I is 8.

The information entropy values of wheat encryption images in Gaoping City in each scheme are shown in Table 10. The entropy value of scheme 1 to scheme 8 is 7.999, which is closest to 8, and has good anti-entropy attack ability. Scheme 9 has the lowest entropy, the smaller the uncertainty, and the worst effect of anti-entropy attack.

Table 10. Information entropy of wheat encryption images.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
Entropy	R	7.999	7.999	7.999	7.999	7.999	7.999	7.999	7.999	7.934	7.987
	G	7.999	7.999	7.999	7.999	7.999	7.999	7.999	7.999	7.934	7.986
	B	7.999	7.999	7.999	7.999	7.999	7.999	7.999	7.999	7.933	7.986

4.6. Gray Difference Degree

Gray difference degree is used to measure the gray level difference between the original image and the encrypted image [35], and the calculation formula is as follows:

$$GVD = \frac{AN'[GN(\alpha,\beta)] - AN[GN(\alpha,\beta)]}{AN'[GN(\alpha,\beta)] + AN[GN(\alpha,\beta)]} \tag{22}$$

$$GN(\alpha,\beta) = \frac{\sum[G(\alpha,\beta) - G(\alpha',\beta')]^2}{4} \tag{23}$$

where $(\alpha', \beta') = \begin{cases} (\alpha\text{-}1, & \beta) \\ (\alpha\text{+}1, & \beta) \\ (\alpha, & \beta\text{+}1) \\ (\alpha, & \beta\text{-}1) \end{cases}$.

$$AN[GN(\alpha,\beta)] = \frac{\sum_{\alpha=2}^{W-1}\sum_{\beta=2}^{H-1} GN(\alpha,\beta)}{(W-2)(H-2)} \tag{24}$$

where $G(\alpha,\beta)$ is the grayscale value at the (α,β) position. GN is the gray difference degree. AN is the average neighborhood gray difference of the original image. AN' is the average neighborhood

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

gray difference of the encrypted image. The value of GVD is between 0 and 1. 0 means two images that are exactly the same, and 1 means two images that are completely different.

In an image, each pixel has a grayscale value that represents its brightness or color intensity. GVD quantifies the degree of variation between images by calculating the grayscale difference between the original image and the encrypted image.

The GVD values of wheat encryption images in Gaoping City in each scheme are shown in Table 11. Scheme 9 exhibits a large GVD value, which is closest to 1 and has the best effect.

Table 11. GVD value of wheat encryption image.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
GVD	R	0.8909	0.8905	0.8904	0.8905	0.891	0.8903	0.8905	0.8908	0.9054	0.8983
	G	0.8887	0.8894	0.8891	0.889	0.889	0.8891	0.8889	0.8888	0.9039	0.8969
	B	0.8966	0.8961	0.8967	0.8964	0.8963	0.8962	0.8967	0.8964	0.9105	0.9039

4.7. Peak Signal to Noise Ratio

The peak signal to noise ratio (PSNR) is the calculation of the error between the corresponding pixels, which is based on the error-sensitive image quality evaluation [36]. The calculation formula is as follows:

$$\mathrm{MSE} = \frac{1}{\mathrm{H} \times \mathrm{W}} \sum_{s=1}^{\mathrm{H}} \sum_{\gamma=1}^{\mathrm{W}} (\mathrm{X}(s,\gamma) - \mathrm{Y}(s,\gamma))^2 \tag{25}$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{(2^{\mathrm{B}}-1)^2}{\mathrm{MSE}}\right) \tag{26}$$

where MSE is the Mean Square Error of the encrypted image X and the original image Y. H is the height of the image and W is the width of the image. B is the number of pixel bits, generally valued at 8, and the gray level of pixels is 256. The larger the value of PSNR, the smaller the distortion, the smaller the gap between the original image and the encrypted image, and the worse the encryption effect.

The PSNR values of wheat encryption images in Gaoping City in each scheme are shown in Table 12. It can be seen that the PSNR value of scheme 9 is the smallest, which indicates that the greater the gap between the original image and the encrypted image, and the better the encryption effect.

Table 12. PSNR value of wheat encryption image.

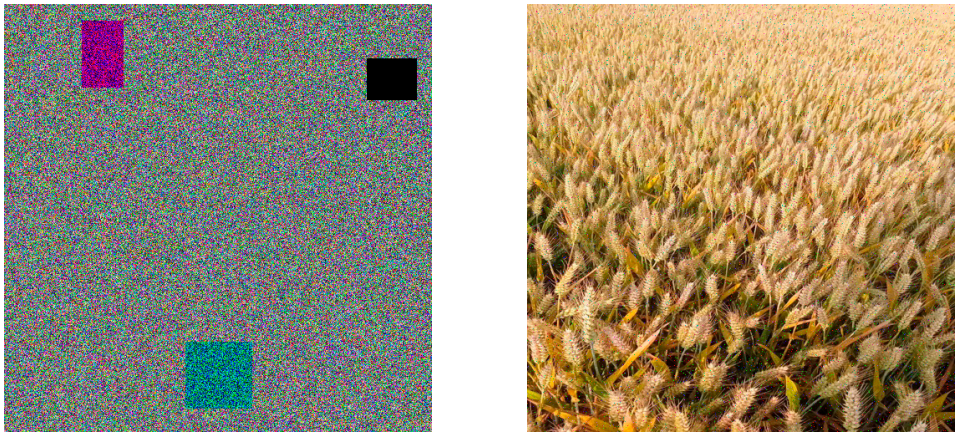
Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
PSNR	R	7.79	7.757	7.809	7.803	7.79	7.806	7.791	7.81	7.37	7.645
	G	8.788	8.738	8.789	8.782	8.776	8.781	8.809	8.783	8.323	8.556
	B	8.399	8.373	8.399	8.412	8.398	8.424	8.397	8.429	8.079	8.122

4.8. Robustness Analysis

Analyze the ability of encrypted images to resist noise attacks and blocking attacks [37]. The encrypted image may be interfered by various factors in the transmission process of the channel, such as blur, distortion and partial information loss. This has an impact on the image decryption effect and increases the difficulty of image decryption.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1

The 60*50 pixels in the encrypted image, the 80*80 pixels in the R channel, and the 50*80 pixels in the G channel are randomly lost. The pixel loss of wheat encryption image in Gaoping City based on scheme 1 is shown in Figure 4(a), and the decrypted result is shown in Figure 4(b). According to the values of NPCR, UACI and PSNR, the anti-blocking ability of encryption algorithm in each scheme is measured, as shown in Table 13. Scheme 9 shows good encryption effect on UACI and PSNR values.



(**a**) (**b**)

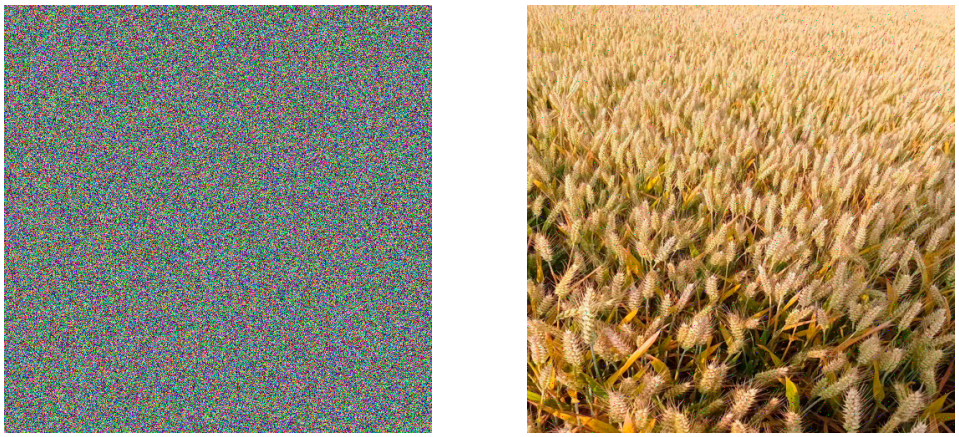
Figure 4. Wheat image encryption with missing pixels. (**a**) Encrypted image; (**b**) Decrypted image.

Table 13. The ability to resist blocking attacks.

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
NPCR (%)	R	99.6059	99.6239	99.6075	99.6132	99.6147	99.5975	99.6113	99.6140	99.6437	99.6185
	G	99.6105	99.6269	99.6025	99.6208	99.6246	99.6380	99.6250	99.6140	99.6441	99.6258
	B	99.6105	99.6117	99.6193	99.6101	99.6300	99.6029	99.6174	99.6124	99.6445	99.6399
UACI (%)	R	31.5418	32.2438	32.2125	32.1892	31.4231	32.1904	32.2455	32.2100	33.7230	32.8882
	G	31.4715	32.2282	32.0488	31.9774	30.8427	32.0953	32.0015	32.0887	33.5209	32.6257
	B	31.4595	32.0328	31.7358	31.7522	33.6116	31.7633	31.6484	31.7250	33.2831	32.3870
PSNR	R	7.568	7.546	7.385	7.577	7.466	7.362	7.472	7.587	7.091	7.227
	G	8.465	8.511	8.693	8.601	8.542	8.488	8.648	8.658	8.171	8.471
	B	8.324	8.332	8.406	8.472	8.418	8.432	8.409	8.462	8.117	8.106

Gaussian white noise with mean 0, standard deviation 1 and variance 1 is added to the encrypted image. The wheat encryption image with white Gaussian noise in Gaoping City based on scheme 1 is shown in Figure 5(a), and the decrypted result is shown in Figure 5(b). According to the values of NPCR, UACI and PSNR, the anti-noise ability of encryption schemes in each scheme is measured, as shown in Table 14. Scheme 8 has good performance on NPCR values, and Scheme 9 shows good encryption effect on UACI and PSNR values.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1431.v1



(**a**) (**b**)

Figure 5. Wheat image encryption with Gaussian white noise. (**a**) Encrypted image; (**b**) Decrypted image.

Table 14. The ability to resist noise attacks

Chaotic System Scheme		1	2	3	4	5	6	7	8	9	10
NPCR (%)	R	99.6059	99.6010	99.6075	99.5918	99.6140	99.6166	99.5987	99.6120	99.6204	99.6212
	G	99.6113	99.6140	99.5956	99.6082	99.5995	99.6277	99.6170	99.6090	99.6258	99.6162
	B	99.6155	99.6162	99.6113	99.6262	99.6288	99.6174	99.6334	99.6113	99.6452	99.6296
UACI (%)	R	31.5531	31.6761	31.4419	31.4250	31.1376	31.4580	31.4930	31.4583	33.1435	32.2366
	G	31.4826	31.6383	31.5071	31.4782	30.0468	31.5326	31.4354	31.5303	33.1200	32.2096
	B	31.4702	31.6361	31.4787	31.5228	33.3605	31.5210	31.4026	31.4969	33.2069	32.2705
PSNR	R	7.772	7.74	7.791	7.785	7.773	7.789	7.774	7.793	7.353	7.629
	G	8.781	8.731	8.782	8.775	8.769	8.774	8.802	8.776	8.315	8.55
	B	8.416	8.389	8.416	8.428	8.415	8.44	8.413	8.445	8.094	8.138

4.9. Experimental summary

In summary, Scheme 9 shows good performance in correlation, UACI value, GVD value, PSNR value, anti-blocking attack ability and anti-noise attack ability. Its key space size is second only to scheme 8 with the largest key space size, but its variance, standard deviation and anti-entropy attack ability are the worst. Scheme 8 shows good performance in key space size, entropy value and anti-noise attack ability. The variance, standard deviation and entropy of scheme 7 are the best. Scheme 1 is closest to the theoretical expected value of NPCR at 99.6094% and has good entropy. Although the key space of scheme 6 and scheme 10 is the smallest, it is much larger than the value that can resist brute force attacks.

5. Conclusions

In this paper, the encryption effects of several common chaotic systems are discussed based on wheat images from Gaoping City, Shanxi Province. Eight common image encryption performance evaluation indexes are histogram analysis, correlation analysis of adjacent pixels, key sensitivity analysis, key space analysis, information entropy analysis, GVD analysis, PSNR analysis and robustness analysis. Through the above analysis, it is found that different chaotic system schemes have different effects on different evaluation indexes and are suitable for different application

scenarios. Among the newly proposed chaotic systems in recent years, such as the new four-dimensional chaotic system represented by scheme 9, the overall encryption effect of wheat encrypted images is good. Because of the high similarity of agricultural images, the new four-dimensional chaotic system can be extended to encrypt other agricultural images. The data presented in section 4 of this paper can also provide references for the selection of encryption schemes for agricultural images.

Author Contributions: Conceptualization, Y.S. and H.Y.; methodology, Y.S. and H.Y.; software, Y.S., X.D. and H.Z.; validation, Y.S., H.Y. and X.D.; formal analysis, Y.S. and H.Y.; investigation, Y.S. and H.Z.; resources, Y.S.; data curation, Y.S.; writing—original draft preparation, Y.S.; writing—review and editing, Y.S.; visualization, Y.S.; supervision, Y.S.; project administration, Y.S.; funding acquisition, Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Postgraduate Scientific Research Innovation Project of Shanxi Province in 2023 (Grant Nos. 2023KY323), the Shanxi Province Basic Research Program Project (Free Exploration) (Grant Nos. 20210302123408), and the Open Project Foundation of Intelligent Information Processing Key Laboratory of Shanxi Province (Grant Nos. CICIP2023002).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The work of this paper is completed under the careful guidance of my supervisor, Professor Yang Hua. Professor Yang has put forward practical guiding suggestions for the article many times, and has revised the article comprehensively and carefully. Here, I would like to express my sincere thanks to Professor Yang!

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ma, H.; Jing, Y.; Huang, W.; Shi, Y.; Dong, Y.; Zhang, J.; Liu, L. Integrating early growth information to monitor winter wheat powdery mildew using multi-temporal Landsat-8 imagery. *Sensors* **2018**, *18*, 3290.
2. Zhao, Y.; Potgieter, A. B.; Zhang, M.; Wu, B.; Hammer, G. L. Predicting wheat yield at the field scale by combining high-resolution Sentinel-2 satellite imagery and crop modelling. *Remote Sensing* **2020**, *12*, 1024.
3. Zhang, J.; Zhao, Y.; Hu, Z.; Xiao, W. Unmanned Aerial System-Based Wheat Biomass Estimation Using Multispectral, Structural and Meteorological Data. *Agriculture* **2023**, *13*, 1621.
4. Yue, X.; Qi, K.; Na, X.; Zhang, Y.; Liu, Y.; Liu, C. Improved YOLOv8-Seg Network for Instance Segmentation of Healthy and Diseased Tomato Plants in the Growth Stage. *Agriculture* **2023**, *13*, 1643.
5. Sánchez Espinosa, K. C.; Fernández-González, M.; Almaguer, M.; Guada, G.; Rodríguez-Rajo, F. J. Puccinia Spore Concentrations in Relation to Weather Factors and Phenological Development of a Wheat Crop in Northwestern Spain. *Agriculture* **2023**, *13*, 1637.
6. Man, Z.; Li, J.; Di, X.; Sheng, Y.; Liu, Z. Double image encryption algorithm based on neural network and chaos. *Chaos, solitons & fractals* **2021**, *152*, 111318.
7. Pourasad, Y.; Ranjbarzadeh, R.; Mardani, A. A new algorithm for digital image encryption based on chaos theory. *Entropy* **2021**, *23*, 341.
8. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 1-39.
9. Zhao, J.; Wang, S.; Zhang, L. Block Image Encryption Algorithm Based on Novel Chaos and DNA Encoding. *Information* **2023**, *14*, 150.
10. Alexan, W.; Elkandoz, M.; Mashaly, M.; Azab, E.; Aboshousha, A. Color image encryption through chaos and kaa map. *IEEE Access* **2023**, *11*, 11541-11554.
11. Zhu, Y.; Wang, C.; Sun, J.; Yu, F. A chaotic image encryption method based on the artificial fish swarms algorithm and the DNA coding. *Mathematics* **2023**, *11*, 767.
12. Premkumar, R.; Mahdal, M.; Elangovan, M. An Efficient Chaos-Based Image Encryption Technique Using Bitplane Decay and Genetic Operators. *Sensors* **2022** , *22*, 8044.
13. Ghadirli, H. M.; Nodehi, A.; Enayatifar, R. An overview of encryption algorithms in color images. *Signal Processing* **2019**, *164*, 163-185.
14. Suneja, K.; Dua, S.; Dua, M. A review of chaos based image encryption. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) **2019**, 2019, 693-698.

15. Roy, S.; Shrivastava, M.; Pandey, C. V.; Nayak, S. K.; Rawat, U. IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata. *Multimedia Tools and Applications* **2021**, *80*, 31529-31567.
16. Khan, P. W.; Byun, Y. A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy* **2020**, *22*, 175.
17. Zhang, Y.; Tang, Y. A plaintext-related image encryption algorithm based on chaos. *Multimedia Tools and Applications* **2018**, *77*, 6647-6669.
18. Zhu, S.; Deng, X.; Zhang, W.; Zhu, C. Image encryption scheme based on newly designed chaotic map and parallel DNA coding. *Mathematics* **2023**, *11*, 231.
19. Santhosh, J.; Balamurugan, P.; Arulkumaran, G.; Baskar, M.; Velumani, R. Image driven multi feature plant management with FDE based smart agriculture with improved security in wireless sensor networks. *Wireless Personal Communications* **2022**, *127*, 1647-1663.
20. Perumal, B.; Ganeshan, A.; Jayagopalan, S.; Preetha, K. S.; Selamban, R.; Elangovan, D.; Balasubramani, S. Real time multi view image based FPC plant management with SS data security and low rate attack detection for efficient smart agriculture in WSN. *Journal of Intelligent & Fuzzy Systems* **2023**, *44*, 91-100.
21. Kulalvaimozhi, V. P.; Alex, M. G.; Peter, S. J. A novel homomorphic encryption and an enhanced DWT (NHE-EDWT) compression of crop images in agriculture field. *Multidimensional Systems and Signal Processing* **2020**, *31*, 367-383.
22. Padmapriya, V. M.; Sowmya, B.; Sumanjali, M.; Jayapalan, A. Chaotic Encryption based secure Transmission. *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking* **2019**, *2019*, 1-5.
23. Smith, L. A.; Ziehmann, C.; Fraedrich, K. Uncertainty dynamics and predictability in chaotic systems. *Quarterly Journal of the Royal Meteorological Society* **1999**, *125*, 2855-2886.
24. Zhao, Y.; Gao, C.; Liu, J.; Dong, S. A self-perturbed pseudo-random sequence generator based on hyperchaos. *Chaos, Solitons & Fractals: X* **2019**, *4*, 100023.
25. Wang, S.; Wang, C.; Xu, C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. *Optics and Lasers in Engineering* **2020**, *128*, 105995.
26. Chen, X. T.; Bao, J. H. Complex dynamical properties of a four-dimension periodically-forced hyperchaotic system. *Journal of Dynamics and Control* **2021**, *19*, 8-15.
27. Wang, Z. L.; Niu, H.; Tan, D. C. Analysis, control and circuit implementation of a novel 4D chaotic system. *Dynamical Systems and Control* **2019**, *2*, 129-139.
28. Yan, M. X.; Zhang, P. Coexistence and image encryption of a new four-dimensional chaotic system with hidden attractors. *Journal of Shandong University of Science and Technology(Natural Science)* **2023**, *42*, 113-126.
29. ur Rehman, A.; Liao, X.; Ashraf, R.; Ullah, S.; Wang, H. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik* **2018**, *159*, 348-367.
30. Zhang, X.; Hu, Y. Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding. *Optics & Laser Technology* **2021**, *141*, 107073.
31. Li, C. L.; Zhou, Y.; Li, H. M.; Feng, W.; Du, J. R. Image encryption scheme with bit-level scrambling and multiplication diffusion. *Multimedia Tools and Applications* **2021**, *80*, 18479-18501.
32. Chai, X.; Wu, H.; Gan, Z.; Han, D.; Zhang, Y.; Chen, Y. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. *Information Sciences* **2021**, *556*, 305-340.
33. Zheng, J.; Zeng, Q. An image encryption algorithm using a dynamic S-box and chaotic maps. *Applied Intelligence* **2022**, *52*, 15703-15717.
34. Khalil, N.; Sarhan, A.; Alshewimy, M. A. An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology* **2021**, *143*, 107326.
35. Murali, P.; Niranjana, G.; Paul, A. J.; Muthu, J. S. Domain-flexible selective image encryption based on genetic operations and chaotic maps. *The Visual Computer* **2023**, *39*, 1057-1079.
36. Wang, X.; Chen, S.; Zhang, Y. A chaotic image encryption algorithm based on random dynamic mixing. *Optics & Laser Technology* **2021**, *138*, 106837.
37. Hosny, K. M.; Kamal, S. T.; Darwish, M. M. A color image encryption technique using block scrambling and chaos. *Multimedia Tools and Applications* **2022**, 1-21.