# A high-quality visual image encryption algorithm utilizing the conservative chaotic system and adaptive embedding

Xiaojun Tong a, Xilin Liu a, \*, Miao Zhang a, Zhu Wang b

*a School of Computer Science and Technology, Harbin Institute of Technology, Weihai, 264209, China*

*b School of Information Science and Engineering, Harbin Institute of Technology, Weihai, 264209, China*

∗Corresponding author: liu\_xilin2023@163.com

**Abstract:** Regarding the issue of encrypted images in the channel attracting the attention of attackers and making them vulnerable to attacks. This paper proposes a high-quality visual image encryption algorithm utilizing the conservative chaotic system, two-dimensional compressive sensing, optimization local of binary patterns, and adaptive embedding method. Firstly, a conservative chaotic system with excellent performance and resistance to reconstruction attacks is proposed. Secondly, the pseudo-random sequences generated by the chaotic system dynamically generate measurement matrices, which are optimized before compressing the image. Then, during the encryption process, by utilizing the newly proposed composite DNA computing rules, chaotic sequences dynamically encode and compute image information, which enriches the coding criteria and improves the security of encryption algorithms. Finally, in the information embedding stage, the newly proposed OLBP algorithm can identify important textured and non-textured regions of the host image, prioritize embedding non-textured regions, and then embed textured regions, which can improve the amount of information embedding and reduce damage to the host image. Experimental simulation and analysis exhibit that the encryption algorithm has high security, strong robustness and high efficiency. Meanwhile the imperceptible analysis of the steganographic images is exceed 52dB, so the algorithm presents a high-quality visual effect of imperceptibility.

**Keywords:** Conservative chaotic system, two-dimensional compressive sensing, optimization local binary pattern, adaptive embedding.

## Introduction

In pace with the speedy expansion of the Internet of Things and information technology, network security has become one of people's common concerns. As the most intuitive and commonly used communication method, the secure dissemination of information through images is crucial. However, illegal acquisition, tampering, and destruction of medical, military, corporate, and personal privacy images often occur, which will cause irreparable losses to society and the entire country. Image encryption is the efficacious measures of protecting image information. Due to the characteristics of images, traditional encryption algorithms are unsuitable for images. Therefore, exploring new image encryption technologies has become a research hotspot. Chaos has an indelible advantage in encryption algorithms due to its unique characteristics [1-4].

Currently, multitudinous chaotic image cryptographic algorithms have been put forward, embodying DNA coding [5-7], Boolean networks or fractal matrix [8-9], compressive sensing [10-12], the model of the cellular automata [13-14], S-box [15-17], new mathematical models [18-19], and so on. Wang et al. [5] proposed a DNA encoding image cryptographic algorithm to achieve the purpose of encrypting images. Yet, Liu et al. [7] designed a dynamic DNA encoding and computation image encryption algorithm, whose dynamic behavior is controlled by sequences generated by chaotic systems. An asynchronous renewal Boolean network encryption algorithm using chaos was put forward by Gao et al. [8]. Xian et al. [9] raised a fractal sorting matrix using spiral transform and applied it to image encryption. To reduce the consumption of information in the channel, Nan et al. [10] and Liu et al. [12] put forward compressed sensing image encryption algorithms, which can achieve both encryption and compression of image information simultaneously. Li et al. [13] present a novel image cryptographic algorithm using cellular automata and composite chaos map. A visualized multiple image selection encryption algorithm using multilayer cellular automata saliency detection was proposed by Su et al. [14]. Zhu et al. [15] and Su et al. [16]. both advanced dynamic S-box image encryption algorithms, which typically require optimization of the S-box. Hence, these algorithms have high security but high time and resource consumption. To improve the safety of the algorithm, Erkan et al. [18] and Toktas et al. [19] have designed image cryptographic algorithms using new mathematical models. These algorithms have low efficiency. As mentioned, notwithstanding the advanced algorithms all reach the aim of image encryption, there are generally some things that could be improved. Firstly, dissipative chaos maps, which exist attractors in the phase space, are used, and destroyers can effectively attack them through reconstruction, which poses a security risk to the encryption algorithm. Secondly, these algorithms encrypt images into noise-like images, which will attract the attacker's attention and make them more vulnerable to attacks.

To overcome the aforementioned drawbacks, many visual security image algorithms have been proposed successively, which can achieve dual protection of images in terms of content and visual aspects [20-21]. Yin et al. [22] drew an image reversible data hiding algorithm using bit-plane compression and pixel prediction, but this scheme has strict requirements for the size of hidden information and can only hide very small amounts of information. A cross-plane thumbnail preservation image encryption scheme was proposed by An et al. [23], and a high-quality visually color image cryptographic algorithm using block compressed sensing and a method of particle swarm optimization was proposed by Chai et al. [24]. These schemes are all aimed at color image encryption and have efficient advantages but lack universality. Huang et al. [25] and Zhu et al. [26] both process plain and carrier images in the frequency domain before embedding, but the embedding position is fixed or related to the key, so the security is unstable. Numerous senior scholars have proposed adaptive image encryption schemes to prevent the embedding position from affecting the safety of the algorithm [27-31]. Long et al. [27] put forward a dynamic matching algorithm in which an adaptive embedding method on account of image energy is raised, improving the implementation of data storage and distributed management. Yang et al. [30] present a visually cryptographic algorithm in which the original image is encrypted and dynamically embedded into the integer wavelet subbands of the host image. To ensure the complete information content of decrypted images, many scholars have proposed lossless compression encryption methods [32-34]. For instance, Yin et al. [32] used the lossless compression method of Huffman encoding, and Yang et al. [34] employed the SHIFT lossless compression method. Nevertheless, these schemes require high requirements for embedding methods and carrier images.

Motivated by the above analysis, we present a high-quality visual image cryptographic algorithm employing a conservative chaotic system, 2D compressive sensing, and adaptive embedding in this paper. First of all, the encryption algorithm employs a conservative chaotic system that can resist reconstruction attacks. Secondly, the sequences produced by the chaotic system dynamically produce compressive sensing measurement matrices. In addition, new composite DNA computation rules are proposed, and the chaotic sequences dynamically control the encoding and computation of DNA rules to achieve image encryption. Finally, in the hiding stage, the OLBP algorithm is used to process the carrier image, identifying important textured and non-textured areas of the carrier image. By embedding the non-textured regions first and then the textured regions, the damage to the host image is reduced, achieving the goal of image visual security. The detailed contributions of the proposed work are listed as follows:

1. Stem from the generalized Sprott-A system, a new conservative chaotic system is proposed, which does not exist attractors and can resist reconstruction attacks. Moreover, the produced sequence has strong pseudo randomness, making it advantageous for application in encryption algorithms.
2. A new method for optimizing the compressive sensing measurement matrix has been proposed. The sequences produced by the chaotic system dynamically produce compressive sensing measurement matrices and then compress the image.
3. The composite DNA computing rules are proposed during the encryption process. The sequences produced by the chaotic system dynamically DNA encode and calculate image information to generate cipher images.
4. At the stage of embedding, the newly proposed optimized local binary pattern (OLBP) algorithm processes the host image, separates important textured and non-textured regions of the image by embedding encrypted information into non-textured regions first and then texture regions to reduce damage of the host image, achieving the goal of imperceptible visual security.

The remainder of this paper is organized as follows. In Section 2, the contribution of the works is introduced. Section 3 presents a detailed algorithm description of the proposed visual image encryption. In Section 4, experimental results and analysis are provided. Conclusions are drawn in Section 5.

## 2. The conservative chaotic system and adaptive embedding algorithm

### 2.1 Design and analysis of a novel conservative chaotic system

**(1) Generalized Sprott-A system**

Sprott introduced several simple 3D chaotic systems in 1994, one of which was deeply studied as the Sprott-A system, and its mathematical representation is described as [35]:



In essence, the Sprott-A system is an exceptional circumstance of the Nosé-Hoover thermostatted oscillator, which has complex, chaotic behavior [36]. Typically, transforming the system into a Kolmogorov system can help analyze the system's dynamic behavior, identify the causes of chaos, and study the impact of energy changes on system dynamics.

Additionally, the Sprott-A system can be described as the Kolmogorov system as follows:



where

, , , and .

Stem from the generalized Sprott-A system, we will introduce a universally applicable method for constructing conservative chaotic systems.

**(2) The conservative chaotic system**

First of all,



Besides,



And,



Let , ,,. Finally, one can get the four dimensional (4D) chaotic system:



**(3) The performance analysis of the proposed system**

For the analysis of chaotic systems, including conservatism analysis, Lyapunov exponent analysis, trajectory analysis, and chaotic sequence analysis. These analyses prove that the system has security advantages in practical applications.

**1) Conservatism analysis**

The chaotic system’s amount of Hamilton energy is



Furthermore,



Consequently, we can obtain:



Evidently,



The Hamilton energy of the 4D chaotic system is always conserved, assuming , the energy of the 4D chaotic system moves on hyperplane *K* invariably. Assuming *a*=2, *b*=3, *c*=1, d=2, the energy diagram of the system is drew as Figure 1.

|  |  |
| --- | --- |
|  |  |
| (a) x1(0)=1, x2(0)=2 | (b) x3(0)=1, x4(0)=2 |
| **Figure 1.** The energy diagram | |

Obviously, when the initial values are given, the energy has already been determined as a fixed value, expressing that the system's energy has always been conserved over time.

In addition, the 4D chaotic system’s divergence is obtained as follows:



where ,,,.

Furthermore, we can get



It is noteworthy that the volume of the 4D chaotic system over time is related to . Assuming that the initial volume of the system is , and when , the volume is



Apparently, the volume of the system is conserved forever.

**2) Lyapunov exponents (LEs) analysis**

When the parameter values , , , , , and initial values *x*1=8, *x*2=6, *x*3=4, *x*4=2, the LEs chart of the chaotic system is described in Figure 2.

|  |
| --- |
|  |
| **Figure 2.** The *LE*s chart |

Through the analysis, we can obtain *LE*1= 24.80, *LE*2= 0.03, *LE*3= -0.04, *LE*4= -24.79. Hence, the system can generate chaotic behavior.

Additionally,



The sum of all *LE*s values is 0, demonstrating that the proposed system has conservative characteristics.

**3) Trajectory analysis**

Analyzing the trajectory of a system can observe its motion behavior in phase space. When initial values (2, 4, 2, 4) and (10, 9, 8, 6) are selected respectively, the flow chart of the 4D conservative chaotic system is drew in Figure 3. In addition, The Poincare section diagram of the system is displayed in Figure 4.

|  |  |
| --- | --- |
|  |  |
| (a) x1-x4 plane | (b) x2-x3 plane |
| **Figure 3.** The flow chart | |

Evidently, the chaotic flow chart produced by the system has to do with the given initial value. When different initial values are chosen, the system produces different chaotic flows, which is also the advantage of conservative chaos.

|  |  |
| --- | --- |
|  |  |
| 1. x1-x2 plane | (b) x1-x2-x4 plane |
| **Figure 4.** The Poincare section diagram | |

From Figure 4, it is clear that the system forms a dense and irregular set of points on the plane, manifesting that it is difficult to determine the system’s behavior.

**4) Sequence analysis**

In general, the National Institute of Standards and Technology (NIST) SP800-22 is employed to test the randomness of the sequence, which consists 15 sub tests. For significance level , the pass rate *T* is



where , , *s* represents dividing into 100 groups. Therefore, if the P-value obtained is within the boundary of and the pass rate *T* is bigger than 0.9602, denoting that the test has been passed.

First of all, iterate the 4D conservative chaotic system to produce sequences *X*1, *X*2, *X*3, *X*4, and then merge them according to the following equation.



Afterwards, perform NIST testing on the chaotic sequence *Y*. and the Figure 5 displays the P-value and pass rate of *Y*.

|  |  |
| --- | --- |
|  |  |
| (a) P-value | (b) Pass rate |
| **Figure 5.** The NIST diagram | |

Through sequence analysis, it is obvious that the chaotic sequence passed all 15 NIST sub-tests, manifesting that the randomness of the sequence can be guaranteed and meet the requirements for subsequent encryption use.

**5) Comparative analysis of the performance of different chaotic systems**

We summarize the performance of the proposed conservative hyperchaotic system and compare it with the emerging hyperchaotic systems and conservative chaotic systems in the current field. Table 1 lists the performance comparison among different chaotic systems. The content of comparison and analysis includes the type of chaotic system, whether the volume of the chaotic system is conservative, whether the energy of the chaotic system is conservative, whether the chaotic system has the ability to resist reconstruction attacks, and whether the chaotic system is hyperchaotic.

**Table 1.** The performance comparison among different chaotic systems

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Algorithms | Type | Conservative volume | Conservative energy | Resist reconstruction attacks | Hyperchaotic system |
| Ref. [1] | Dissipative | × | × | × | √ |
| Ref. [37] | Dissipative | × | × | × | √ |
| Ref. [38] | Dissipative | × | × | × | √ |
| Ref. [39] | Dissipative | × | × | × | √ |
| Ref. [40] | Conservative | × | × | √ | × |
| Ref. [41] | Conservative | × | √ | √ | √ |
| Ref. [42] | Conservative | √ | √ | √ | × |
| Ref. [43] | Conservative | √ | √ | √ | × |
| Proposed chaotic systems | Conservative | **√** | **√** | **√** | **√** |

As can be seen from Table 1, the proposed system is a Hamiltonian hyperchaotic system with both conservative volume and energy. This system not only has a huge key space, but also has the conservativeness of energy and volume, as well as the ability to resist reconstruction attacks. Compared with the recently proposed hyperchaotic and conservative chaotic systems, the proposed conservative hyperchaotic system exhibits more advantages.

### 2.2. The compressive sensing algorithm

Typically, there is redundancy in signals, and the complexity of signals can be reduced by compressing their information. Compressive sensing (CS) is a new signal compression method recently proposed, which can reconstruct the original signal with fewer sampled signals compared to traditional Nyquist sampling [44].

For a sparse signal *S* with a size of  can be measured as [45]:



where  is an  orthogonal basis, and , which denotes the measurement matrix. Afterwards, transposition of  in the  domain,  can be obtained as:



where .

Therefore, the two-dimensional (2D) CS can be defined by another measurement matrix  as:



where , which denotes another measurement matrix, and , which represents the measurement value matrix.

Supposing that  and  meet the restricted isometry property (RIP), the original signal *S* may be accurately reconstructed from *Z* by handling the optimal problem, the detail problem is as follow:



where denotes the  norm of the vector *S*.

Recently, multitudinous learned researchers have introduced many excellent methods for signal recovery, such as MP, OMP, SL0, 2DPG-ED, and so on. Among them, 2DPG-ED [46] has more advantages in signal recovery, so this paper chooses this method for signal recovery.

### 2.3 The optimization local binary pattern algorithm

The local binary pattern (LBP) is a texture description operator with the advantages of rotation invariance and grayscale invariance, first proposed by Ojala et al. in 1996 [47]. This algorithm displays the texture features of a particular part by describing the pixel relationship between the pixel in that position and its surrounding eight adjacent neighborhoods.

To maximize the display of the most essential texture in the image, we propose an optimized local binary pattern (OLBP) algorithm based on the traditional LBP algorithm. This method gives priority to embedding pixel positions that are not essential textures, followed by embedding the positions of texture pixels. On the one hand, this can expand the capacity of subsequent pixel embeddings. On the other hand, it minimizes the impact on the carrier image to the greatest extent possible. The operation process of the OLBP algorithm is described in Figure 6. The specific steps are as follows:

|  |
| --- |
|  |
| **Figure 6.** The operation of OLBP |

**Step 1.** Select a pixel block of size in the image, where the intermediate pixel value is  and the surrounding pixels are .

**Step 2.** Calculate the threshold . 

**Step 3.** Modify the pixel values around position . .

**Step 4.** If the modified  value is less than the , its pixel value is installed to 0; if not, it is installed to 1.

**Step 5.** Combine the obtained values in a clockwise direction into an 8-bit binary number and convert it to a decimal value as the final pixel value.

**Step 6.** Repeat steps 1 to 5 for all values of the image pixel to obtain the OLBP processed matrix.

Figure 7 shows the OLBP operation of the Butfish image.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 1. Butfish | (b) LBP image of Butfish | (c) OLBP image of Butfish |
| **Figure 7.** OLBP operation of Butfish image | | |

The OLBP algorithm selects important texture regions of the Butfish image, and non-texture regions are labeled as black areas. When performing information hiding, the adaptive information hiding algorithm can significantly improve the capacity of the carrier image and reduce damage to the carrier image by first embedding non-textured regions and then embedding textured regions.

### 2.4 The composite DNA computing algorithm

Typically, DNA sequences are composed of four bases, embodying adenine (A), thymine (T), cytosine (C), and guanine (G), where C and G, A and T are complementary. Each image pixel value is transformed into an 8-bit binary, and an 8-bit binary sequence can be converted into a DNA sequence. The encoding rules are shown in Table 2. After encoding, DNA calculations can be performed to reach the aim of encryption. For example, if the pixel value is 228, it is converted to binary as (11100100)2 and encoded on the basis of Rule 1 in Table 2, and it can be represented as TGCA.

**(1) DNA coding rulers**

**Table 2.** The eight coding rulers

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code | R 1 | R 2 | R 3 | R4 | R 5 | R 6 | R 7 | R 8 |
| 11 | T | T | G | G | C | C | A | A |
| 10 | G | C | T | A | T | A | G | C |
| 01 | C | G | A | T | A | T | C | G |
| 00 | A | A | C | C | G | G | T | T |

**(2) The traditional computing methods**

The traditional computing methods for DNA typically include three types: addition, subtraction, and XOR. Table 3 shows the DNA sequence addition rulers.

**Table 3.** Addition rulers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Add | A | C | G | T |
| T | T | G | A | C |
| C | C | A | T | G |
| G | G | T | C | A |
| A | A | C | G | T |

Table 4 describes the rules for DNA sequence subtraction.

**Table 4.** Subtraction rulers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sub | A | C | G | T |
| T | T | G | C | A |
| C | C | A | G | T |
| G | G | T | A | C |
| A | A | C | T | G |

And the DNA sequence XOR rulers are illustrated in Table 5.

**Table 5.** XOR rulers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| XOR | A | C | G | T |
| T | T | G | C | A |
| C | C | A | T | G |
| G | G | T | A | C |
| A | A | C | G | T |

In order to further enrich the computing rules of DNA sequences, we will introduce the newly designed composite computing rules later.

**(3) New composite DNA computing methods**

Based on traditional calculation methods, we have designed new composite DNA computing methods, but these computing methods need to meet the following rules:



The rules require that the value of the element remains unchanged every four rounds or multiples of 4. Otherwise, the element will change. Figure 8 illustrates three newly designed DNA computing rules.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| (a) Add~ operation | (b) Sub~ operation | (c) XOR~ operation |
| **Figure 8.** The diagram of composite computing rulers | | |

Among them, the Add~ rules of DNA sequences are depicted in Table 6.

**Table 6.** Add~ rulers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Add~ | A | C | G | T |
| T | C | A | G | T |
| C | T | G | C | A |
| G | A | C | T | G |
| A | G | T | A | C |

The Sub~ rules of DNA sequences are displayed in Table 7.

**Table 7.** Sub~ rulers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sub~ | A | C | G | T |
| T | G | T | A | C |
| C | A | C | T | G |
| G | T | G | C | A |
| A | C | A | G | T |

And the XOR~ rules of DNA sequences are described in Table 8.

**Table 8.** XOR~ rulers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| XOR~ | A | C | G | T |
| T | A | C | T | G |
| C | T | G | A | C |
| G | C | A | G | T |
| A | G | T | C | A |

The process of generating ciphertext using a  plaintext matrix is shown in Figure 9.

|  |
| --- |
|  |
| **Figure 9.** The simulation of information encryption |

It is apparent that the cipher information is entirely different from the plain information.

## 3. The visual image encryption algorithm utilizing adaptive embedding

This section intoroduces a detailed introduction to the implementation process of visual image encryption and decryption.

### 3.1 The model of the visual cryptographic algorithm

Figure 10 depicts the model chart of the visual cryptographic algorithm.

|  |
| --- |
|  |
| **Figure 10.** The chart of encryption algorithm |

Apparently, the proposed cryptographic algorithm mainly includes two stages: the first stage is the compression and encryption process, and the second stage is the process of adaptive embedding of images.

### 3.2 The process of the visual image cryptographic algorithm

#### 3.2.1 The process of encryption and compressive

**(1) Initial keys generation**

**Step 1.** Enter a plaintext image *P* with a size of , and calculate the image

employing SHA-512 and produce a 512-bit hash value *H*. Afterwards, convert *H* to decimal *K*.

**Step 2.** Input the initial values of the conservative chaotic system, , , , . And the final initial values of the system can be further obtained from the followings:



And the parameter value  is



where *mod* represents taking remainder, and *round* represents taking multiple rounded decimals.

**(2) The process of initial scramble**

Input the initial value of the system , parameter value , and iterate the system  times to produce sequences , where , and among them,  is for the system to skip the transition state. Subsequently, Perform non-repetitive initial scrambling on the image according to the followings:



Furthermore,



Afterwords, sort the sequence without repetition, as follows:



and



Finally, unfold the image into a one-dimensional vector , and then scramble it according to the followings:



where .

**(3) The process of 2D CS**

Then, by iteratively the proposed chaotic system using different initial values and control parameters at each sampling interval , sequences  and  can be obtained, where *CR* is the compression rate. It means that the system has been iterated by times. Then, according to the following equations to obtain two sequences  and :



Furthermore, the measurement matrices and  can be obtained by the followings:



and



Afterwords, cipher  can be obtained by the followings:



Finally, the image is quantized to get cipher , and to limit the value of the output matrix after compressed sensing measurement to the scope of [0, 255], image processing is required, and the process as follows:



where  is the minimum value in , and  is the maximum value in . and  represents rounding a number to an integer.

**(4)** **The process of secondary encryption**

Firstly, obtain the size of , as follows:



and



Besides, according to the following equations, obtain pseudo-random sequences:



Convert  back to  size, and



Further convert the image to binary and generate a matrix  with a size of , and dynamically rotate the image. The specific operation is as follows:



and



where *circshift* represents a cyclic shift operation.

According to the sequence ,  and  are dynamically encoded to generate DNA sequences  and , as shown in Table 1.



Based on the value of sequence , sequences  and  dynamically select calculation rules to generate ciphertext , whose calculation rules are shown in Tables 2, 3, 4, 5, and 6.

#### 3.2.2 The process of adaptive embedding

**(5) Preprocessing of carrier image**

Enter a host image *D* with a size of , and perform OLBP algorithm on image *D* to get image *D1*.The detailed operation is present in Algorithm 1.

|  |
| --- |
| **Algorithm 1.** Production of the OLBP matrix *D1* |
| **Input:** carrier image *D*.  1: Divide the matrix *D* intoblocks with values , .  2: for *i* = *M*1-1  3: for *j* = *N*1-1  4: neigh= [*P* (*i*-1, *j*-1), *P* (*i*-1, *j*), *P* (*i*-1, *j*+1), *P* (*i*, *j*+1), *P* (*i*+1,  5: *j*+1), *P* (*i*+1, *j*), *P* (*i*+1, *j*-1), *P* (*i*, *j*-1),]  6: *t*=min (neigh, *P* (*i*, *j*))  7: neigh= [abs (neigh- *P* (*i*, *j*))]  8: if neigh > *t*  9: pi\_value = 1  10: else  11: pi\_value = 0  12: end if  13: for t =1: 8  14: pi\_value =pi\_value + neigh (1, k)bitshift (1, 8-t)  15: end for  16: *D*1(i, j) = pi\_value  17: end for  18: end for  **Output:** TheOLBP matrix *D1*. |

**(6) The process of adaptive embedding**

Generate the binary matrix *DD* according to the following equations:



In view of the above method, the textured and non-textured regions of the host image are obtained. To reduce damage to the host image, we first embed the ciphertext image into the non-textured area of the host image and then choose to embed the remaining ciphertext information into the textured area.

Convert each pixel value of the host image into an 8-bit binary *D*2, and convert the ciphertext *C*7 into a binary sequence. Based on the value of binary *DD,* we first embed the ciphertext image into the last bit of the binary pixel value in the non-textured area of the host image *D*2. If there is any remaining ciphertext image information, we embed it into the last bit of the binary pixel value in the textured area of the host image. In the end, we obtained visual safety image *D*3.

### 3.3 The model of the visual decryption algorithm

The model diagram of the visual decryption algorithm is described in Figure 11.

|  |
| --- |
|  |
| **Figure 11.** The diagram of decryption algorithm |

Consequently, the proposed decryption algorithm mainly consists of two stages: the first stage is the adaptive extraction and decryption of the image. The second stage is the reconstruction and anti-scramble process of images. The detailed decryption process is the inverse of the encryption and will not be elaborated on here.

## 4. Experimental results and analysis

To verify the feasibility and high quality of the visual cryptographic algorithm, all the experiment tests are operated on a desktop computer with 3.00 GHz, 16 GB RAM, Intel Core i5-9500 CPU, and the operating system is Microsoft Windows 10. In addition, the initial key [*x*1(0), *x*2(0), *x*3(0), *x*4(0)] is set to [0.1, 0.2, 0.3, 0.4], and the parameter value [*a*, *b*, *c*, *d*, *k*] is set to [2, 1, 2, 1, 3], and the compression ratio *CR* = 0.5, *d* = 25.

### 4.1 Encryption and decryption test

Simulation experiments are operated to check the proposed visual image cryptographic algorithm. Foremost, we have selected multiple images to perform in ChestX-ray14 database, USC-SIPI database, CVG-URG database, etc. This includes various scene images, as well as various sizes, grayscale, and color images, and the test results are displayed in Figure 12.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) Medical image 1 | (b) Medical image 2 | (c) Lena | (d) Leopard |
|  |  |  |  |
| (e) Compression encryption of (a) | (f) Compression encryption of (b) | (g) Compression encryption of (c) | (h) Compression encryption of (d) |
|  |  |  |  |
| (i) Host image Baboon | (j) Host image Butfish | (k) Host image Car | (l) Host image Cactusfl |
|  |  |  |  |
| (m) Cipher image Baboon | (n) Cipher image Butfish | (o) Cipher image Car | (p) Cipher image Cactusfl |
|  |  |  |  |
| (q) Reconstruction image of (e) | (r) Reconstruction image of (f) | (s) Reconstruction image of (g) | (t) Reconstruction image of (h) |
| **Figure 12.** The test of encryption and decryption | | | |

From Figure 12, it is obvious that the algorithm can achieve the aim of encryption and decryption for both grayscale and color images, as well as medical and human images, etc. Moreover, the host image embedded with encrypted information cannot be distinguished from the plain image, and the decrypted and decompressed image cannot be distinguished from the plain image, thus achieving visual security.

### 4.2 The quality analysis of the construction and embedding

Additionally, in order to objectively and fairly evaluate the quality of the simulation results, the peak signal-to-noise ratio (PSNR) and the mean structural similarity (MSSIM) are usually employed to estimate the quality of ciphertext images and reconstructed images. The detailed formulas are described in [20].

Consequently, Table 9 lists the PSNR and MSSIM values between the reconstructed image and the original image, as well as the host image and the steganographic image.

**Table 9.** The result of the PSNR and MSSIM values

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Plain image | Host image |  |  |  |  |
| Lena | Baboon | 38.8878 | 0.9782 | 52.8842 | 0.9995 |
| Female | Peppers | 40.4088 | 0.9793 | 52.8962 | 0.9975 |
| Einstein | Boat | 36.6366 | 0.9454 | 52.8951 | 0.9956 |
| Clock | Car | 38.1366 | 0.9761 | 52.9168 | 0.9971 |
| Elaine | Airplane | 35.0635 | 0.9319 | 52.8959 | 0.9956 |
| House | Lake | 39.4654 | 0.9714 | 52.8939 | 0.9977 |

According to Table 9, the PSNR of the carrier image and the steganographic image are about 52.8970, and the MSSIM is about 0.9972, manifesting that these two images are approximately the same, and the embedding of encrypted information has little impact on the host image. Additionally, the PSNR of the original image and the reconstructed image is about 38.0998, and the MSSIM is about 0.9637, indicating that the decompressed image is almost identical to the original image. This all implies that the algorithm we designed exists outstanding compression and hiding effects.

Meanwhile, we tested the decryption performance of the cryptographic algorithm under different CR conditions and the damage to the carrier image. Using Baboon as the carrier image and selecting different images as encryption information, the results are shown in Figure 13. Selecting tipo4\_e image as encrypted information and different images as carriers to test, and the results obtained are displayed in Table 10.

|  |
| --- |
|  |
| **Figure 13.** The PSNR values of different encryption information |
| When selecting different encrypted images and a particular host image, we find that even with different CR values, the algorithm can still achieve larger PSNR values, indicating that the algorithm has universal applicability to encrypted images and will not reduce performance due to specific images. |

**Table 10.** The PSNR values of different carrier images (unit: dB)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Plain image | Host image | CR | | | |
| 0.25 | 0.5 | 0.75 | 0.9375 |
| tipo4\_e | Peppers | 64.7433 | 58.8462 | 55.3995 | 53.4526 |
| Car | 64.6630 | 58.8464 | 55.3854 | 53.4526 |
| Lake | 64.7130 | 58.8514 | 55.3440 | 53.4610 |
| Baboon | 64.7493 | 58.8373 | 55.3875 | 53.4321 |

It is apparent that when the encrypted image is fixed, and different host images are selected, the algorithm still obtains excellent PSNR values under different CR conditions, showing little impact on the carrier image, indicating that the algorithm has universal adaptability to the host image and can achieve high-quality hiding effects.

For the comparison reconstructed images quality, we used the PSNR indicator as the main analysis indicator, and the PSNR results are displayed in Table 11, where *N* manifests that it is not offered in the literature.

**Table 11.** The PSNR values of reconstructed images

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Plain image | Host image | *PSNR* | | | | |  |
| Ref. [48] | Ref. [49] | Ref. [55] | Ref. [56] | Ours | |
| Lena | Peppers | 32.15 | 39.7910 | 33.0984 | 32.9538 | 38.8878 | |
| Female | Airplane | 32.96 | *N* | *N* | *N* | 40.4088 | |
| House | Sailboat | *N* | 33.0946 | 32.9378 | 31.9479 | 39.4654 | |
| Boat | Barbara | *N* | 32.2650 | 32.2659 | 32.2659 | 33.4186 | |
| Clock | Car | *N* | *N* | *N* | *N* | 38.1366 | |
| Airplane | Baboon | *N* | *N* | *N* | *N* | 41.9548 | |
| **Average** |  | **32.5550** | **35.0502** | **32.7674** | **32.3892** | **38.7120** | |

It is clearly that the average PSNR of our designed algorithm is about 38.7120, which is much better than that of other algorithms, manifesting that the algorithm has excellent compression encryption and reconstruction effects.

For the steganographic image quality, we still employed PSNR and MISSM indicators as the primary analysis indicators, and the PSNR results are displayed in Table 12.

**Table 12.** The PSNR values of steganographic images

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Plain image | Host image | *PSNR* | | | |  |
| Ref. [49] | Ref. [55] | Ref. [56] | Ref. [57] | Ours |
| Lena | Baboon | 47.2248 | 35.1636 | 35.4068 | 32.3513 | 52.8842 |
| Female | Airplane | *N* | *N* | *N* | 37.8967 | 52.8964 |
| House | Sailboat | 47.2754 | 36.8192 | 36.9968 | *N* | 52.8943 |
| Boat | Barbara | 47.2759 | 35.9146 | 35..977 | *N* | 52.8787 |
| Clock | Car | *N* | *N* | *N* | *N* | 52.9168 |
| Airplane | Baboon | *N* | *N* | *N* | 35.5629 | 52.9127 |
| **Average** |  | **47.2587** | **35.9658** | **36.2888** | **35.2703** | **52.8972** |

We can find that the mean PSNR of the steganographic image is 52.8972, which is much better than other algorithms. In addition, the MSSIM results are shown in Table 13.

**The 13.** The MSSIM values of steganographic images of different algorithms

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Plain image | Host image | *MSSIM* | | | |  |
| Ref. [49] | Ref. [55] | Ref. [56] | Ref. [57] | Ours |
| Lena | Baboon | 0.9983 | 0.9941 | 0.9973 | 0.9257 | 0.9995 |
| Female | Airplane | *N* | *N* | *N* | 0.9666 | 0.9976 |
| House | Sailboat | 0.9969 | 0.9904 | 0.9965 | *N* | 0.9975 |
| Boat | Barbara | 0.9971 | 0.9872 | 0.9945 | *N* | 0.9978 |
| Clock | Car | *N* | *N* | *N* | *N* | 0.9971 |
| Airplane | Baboon | *N* | *N* | *N* | *N* | 0.9978 |
| **Average** |  | **0.9974** | **0.9906** | **0.9961** | **0.9462** | **0.9979** |

From Table 13, we can obtain that the mean SSIM of the steganographic image is about 0.9979, which is also much better than other algorithms. These all manifests that the proposed adaptive embedding algorithm has very little damage to the image of the carrier and meets the requirements of high-quality embedding algorithms.

### 4.3 Key space analysis

The key space of a cryptographic algorithm refers to the sum of all the keys of the algorithm. The key proposed for the algorithm contains the initial value of the system, with each step size of , obtaining a key space of . On the other hand, the key is the 512-bit hash value of the image, so the key space size is . Consequently, the key space of the algorithm is about . Moreover, the key space for the recently proposed cryptographic algorithm is shown in Table 14.

**Table 14.** The key space of recently cryptographic algorithms

|  |  |
| --- | --- |
| Algorithms | Key space |
| Ref. [48] | 2376 |
| Ref. [49] | About 2418 |
| Ref. [50] | 2149 |
| Ref. [51] | About 2294 |
| Ref. [52] | 2446 |
| Ours | 2712 |

The algorithm's key space is much larger than the required value 2100 and other excellent algorithms, presenting sufficient key space and advantages in resisting brute force attacks.

### 4.4 Histogram analysis

The histogram of image information can display the distribution of image pixels. In this section, when the CR is 0.5, we calculate the histograms of the original image and the cipher image, as well as the host and steganographic images. Figure 14 and 15 respectively describe their corresponding test results.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) Female image | (b) Histogram of (a) | (c) Cipher of (a) | (d) Histogram of (c) |
|  |  |  |  |
| (e) Boat image | (f) Histogram of (e) | (g) Cipher of (e) | (h) Histogram of (g) |
| **Figure 14.** The histogram of plain image and the cipher image | | | |

From Figure 14, it is clear that the proposed algorithm's pixel histogram of the encrypted image is evenly distributed and can hide the pixel information of the plaintext image.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) Earth image | (b) Histogram of (a) | (c) Visual image of (a) | (d) Histogram of (c) |
|  |  |  |  |
| (e) Peppers image | (f) Histogram of (e) | (g) Visual image of (e) | (h) Histogram of (g) |
| **Figure 15.** The histogram of host image and the steganographic image | | | |

Similarly, from Figure 15, we can conclude that the host image is similar to the steganographic image and difficult to distinguish with the naked eye. The pixel distribution histogram is also roughly the same, indicating that the proposed algorithm has little impact on the carrier's image and can better achieve visual security.

### 4.5 Information entropy analysis

Information entropy (IE) is one of the important indicators for analyzing the resistance of encryption algorithms to statistical attacks. Greater information entropy declares a higher degree of information uncertainty in digital images. The mathematical expression of the IE is defined in [53].

Equally, when the CR is 0.5, we selected multiple images in the database for experiments, and the corresponding test results are displayed in Figure 16.

|  |
| --- |
|  |
| **Figure 16.** The IE results of multiple images |

From Figure 16, It is evident that although the information content of the compressed image is significantly reduced, and even some plain images have an information entropy of around 1, the information entropy of the encrypted image has always been about 8, demonstrating that the algorithm has an excellent capability to hide plaintext information.

### 4.6 Correlation coefficient analysis

The neighboring pixels in the original image exhibit significant correlation, in which attackers may obtain information about the plaintext. Mastering this information is likely to break through encryption algorithms. Therefore, outstanding encryption algorithms can reduce these correlations, and correlation coefficients (CC) are one way to test this relationship. The detailed formula is described in reference [54].

We randomly selected multiple pairs of pixels in the Frog plain and cipher image and tested their CCs in various directions, such as horizontal, vertical, and diagonal directions. The corresponding results are described in Figure 17. The results of selecting multiple images and their corresponding correlation coefficients are displayed in Figure 18.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) Frog | (b) R plane of (a) | (c) G plane of (a) | (d) B plane of (a) |
|  |  |  |  |
| (e) Cipher of (a) | (f) R plane of (e) | (g) G plane of (e) | (h) B plane of (e) |
| **Figure 17.** The CC results of Frog image | | | |

We can clearly find that the color Frog plain image has a strong correlation and has significantly reduced their correlation after encryption by the algorithm, demonstrating the strong ability of the algorithm to hide ciphertext information.

|  |
| --- |
|  |
| **Figure 18.** The CC results of different images |

From Figure 18, it can be seen that the encryption algorithm has universality for images. Regardless of the amount of information in the image, the encryption algorithm we present can effectively reduce the correlation of image information and protect it well.

### 4.7 Plaintext sensitivity analysis

Plaintext sensitivity aims to analyze the sensitivity of algorithms to plaintext. When the plaintext image information changes slightly, outstanding algorithms are more sensitive, and the generated ciphertext will cause significant changes. Conversely, it indicates that the algorithm is not sensitive to the plaintext information of the image. The number of pixels changing rate (NPCR)and the unified average changed intensity (UACI) can be used as indicators for detecting the sensitivity of algorithms to plaintext information, and the detailed formulas are defined in [28]

After slightly changing the value of a pixel position on different plain images, the NPCR and UACI calculated for the ciphertext image and the original ciphertext image are displayed in Table 15.

**Table 15.** The NPCR and UACI values of two times cipher image (unit: %)

|  |  |  |  |
| --- | --- | --- | --- |
| Plain image | Host image | NPCR | UACI |
| Baboon | Earth | 99.6109 | 33.4933 |
| Boat | Earth | 99.5987 | 33.3820 |
| Airplane | Earth | 99.6063 | 33.5100 |
| Couple | Butfish | 99.6002 | 33.3339 |
| Truck | Butfish | 99.6124 | 33.4424 |

We can obtain an average value of 99.6097% for NPCR and 33.4323% for UACI, close to their theoretical values of 99.6094% and 33.4635%, respectively. This manifests that the algorithm is very sensitive to ordinary image information.

### 4.8 Robustness analysis

Excellent encryption algorithms have robustness, especially in the transmission channel where there may be information loss or salt and pepper noise. Therefore, robustness analysis is conducted on the proposed algorithm in this section.

#### 4.8.1 Cropping attack

In this section, when the CR is 0.5, we select Female, House, and Lena images as encrypted images and Elephant, Earth, and Butfish as steganographic images. The decryption results obtained in the simulated channel with different amounts of information loss in steganographic images are displayed in Figure 19, and the PSNR values are described in Figure 20.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) Elephant 1/2 loss | (b) Elephant 1/4 loss | (c) Elephant 1/8 loss | (d) Elephant 1/16 loss |
|  |  |  |  |
| (e) Decryption of (a) | (f) Decryption of (b) | (g) Decryption of (c) | (h) Decryption of (d) |
|  |  |  |  |
| (i) Earth 1/2 loss | (j) Earth 1/4 loss | (k) Earth 1/8 loss | (l) Earth 1/16 loss |
|  |  |  |  |
| (m) Decryption of (i) | (n) Decryption of (j) | (o) Decryption of (k) | (p) Decryption of (l) |
| **Figure 19.** The results of cropping attacks with different intensities | | | |

The decrypted image can still be obtained even if the steganographic image information is lost in the channel. Even though 50% of the data is lost in the steganographic image, the decrypted image can still be clearly seen, indicating that the algorithm can resist information loss attacks in the channel.

|  |
| --- |
|  |
| **Figure 20.** The PSNR values of cropping attacks with different intensities |

We can observe that the algorithm can still obtain decrypted images and PSNR values exceeding 30 dB for cropping attacks with varying intensities. The algorithm can stand cropping attacks in the channel well.

#### 4.8.2 Noise attack

Similarly, when the CR is 0.5, we select Female, House, and Lena images as encrypted images and Elephant, Earth, and Butfish as steganographic images. The decryption results obtained by adding different salt and pepper noise (SPN) intensities to the steganographic image are described in Figure 21, and the PSNR values are drew in Figure 22.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (a) 0.5% SPN Butfish | (b) 1% SPN Butfish | (c) 5% SPN Butfish | (d) 10% SPN Butfish |
|  |  |  |  |
| (e) Decryption of (a) | (f) Decryption of (b) | (g) Decryption of (c) | (h) Decryption of (d) |
|  |  |  |  |
| (i) 0.5% SPN Earth | (g) 1% SPN Earth | (k) 5% SPN Earth | (l) 10% SPN Earth |
|  |  |  |  |
| (m) Decryption of (i) | (n) Decryption of (g) | (o) Decryption of (k) | (p) Decryption of (l) |
| **Figure 21.** The results of SPN with different intensities | | | |

It is evidently observed that the algorithm can still decrypt the corresponding decrypted images for SPNs with different intensities in the channel, and even with the addition of 10% intensity, the corresponding decrypted images can still be obtained. This further implies that the proposed algorithm has sufficient robustness.

|  |
| --- |
|  |
| **Figure 22.** The PSNR values of cropping attacks with different intensities |

Moreover, from Figure 22, we can find that for SPN attacks with varying intensities, the proposed algorithm can still obtain decrypted images and excellent PSNR values, showing the algorithm's robustness.

For the robustness comparison analysis, the PSNR indicator is also chosen to analyze the robustness of different algorithms, and the PSNR results of data loss are displayed in Table 16.

**Table 16.** The PSNR values of data loss attacks

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Size | *PSNR* | | | | | |
| Ref. [48] | Ref. [52] | Ref. [58] | Ref. [59] | Ref. [60] | Ours |
|  | 31.72 | 32.71 | 33.95 | 30.06 | *N* | 40.60 |
|  | 30.47 | 30.18 | 32.88 | 28.65 | 32.04 | 40.53 |
|  | 29.95 | 29.01 | 32.19 | 28.19 | *N* | 40.48 |
|  | 28.98 | N | 30.42 | *N* | *N* | 40.41 |
|  | *N* | *N* | *N* | *N* | 20.58 | 38.58 |
|  | *N* | *N* | *N* | *N* | 14.68 | 34.45 |

By simulating information loss of different sizes, the algorithm can still obtain larger PSNR values, and the impact of lost information on the algorithm is small. The PSNR values of SPN attacks are displayed in Table 17.

**Table 17.** The PSNR values of SPN attacks

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Attack  intensity | *PSNR* | | | | | |
| Ref. [48] | Ref. [52] | Ref. [55] | Ref. [58] | Ref. [59] | Ours |
| 0.0001% | 33.13 | 28.18 | 33.44 | 35.20 | 28.07 | 40.12 |
| 0.0003% | 33.13 | 28.18 | 33.44 | 34.86 | 28.07 | 39.14 |
| 0.0005% | 33.13 | 28.17 | 33.44 | 34.80 | 28.07 | 38.85 |

From Tables 16 and 17, We can obtain that whether it is a cropping attack with varying intensities or an SPN attack, the calculated PSNR values are all superior to other encryption algorithms, further proving the proposed algorithm's high-quality robustness.

### 4.9 Efficiency analysis

An outstanding encryption algorithm not only needs to have security guarantees but also needs efficiency. Therefore, we selected images of different sizes as encrypted information to calculate the corresponding consumption time of the encryption process, as displayed in Table 18.

**Table 18.** Running time for encryption process (unit: s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Encryption image | Image | Compression and Encryption | Embedding | Total |
|  | Tipo4\_e | 0.1323 | 0.1279 | 0.2602 |
| Tipo4\_f | 0.1280 | 0.1246 | 0.2526 |
|  | Lena | 0.1715 | 0.4829 | 0.6544 |
| Female | 0.1721 | 0.4865 | 0.6586 |
| House | 0.1871 | 0.4749 | 0.6620 |

Consequently, the compression, encryption, and hiding processes of encryption algorithms can be achieved in a very short amount of time. Moreover, the consumption time of the decryption process is displayed in Table 19.

**Table 19.** Running time for decryption process (unit: s)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Encryption image | Image | Extraction | Reconstruction | Total |
|  | Tipo4\_e | 0.1610 | 1.6398 | 1.8008 |
| Tipo4\_f | 0.1546 | 1.4869 | 1.6415 |
|  | Lena | 0.6217 | 4.0207 | 4.6424 |
| Female | 0.6155 | 3.8957 | 4.5112 |
| House | 0.6121 | 3.0979 | 3.7100 |

According to Tables 18 and 19, the primary time consumption of the algorithm is in the reconstruction process, accounting for more than 50% of the total time consumption. Overall, the algorithm is still relatively efficient in each stage and can quickly complete the encryption purpose.

## 5. Conclusions

To ensure the confidentiality of images in the transmission channel, a high-quality, visual image encryption algorithm based on a conservative chaotic system and adaptive embedding is put forward. Firstly, a high-performance conservative chaotic system capable of resisting reconstruction attack is proposed. Secondly, in the encryption and compression stage, 2D compression sensing is used, and a conservative chaotic system dynamically generates measurement matrices for 2D compression sensing and compresses the images. In the encryption stage, new composite DNA computing rules are designed, combined with the sequences produced by the chaotic system, to dynamically encrypt the image. Finally, in the embedding stage, the OLBP algorithm, which can annotate the important texture features of the host image to the greatest extent, is proposed. The encrypted information is first embedded in unimportant non-textured regions and then embedded in texture regions. On the one hand, it can increase the amount of embedded data; on the other hand, it can reduce the damage to the host image information. Experimental simulation and testing imply that the algorithm has excellent encryption, compression, and embedding effects and is a high-quality visual image cryptographic algorithm with practical application value.

**Acknowledgments**

This research was supported by the Natural Science Foundation of Shandong Provincial (Grant No. ZR2019MF054) and the National Natural Science Foundation of China (Grant No. 61902091).

## References

[1] Wu Y R, Zhang L L, Berretti S, et al. Medical image encryption by content-aware DNA computing for secure healthcare, IEEE Transactions on Industrial Informatics, 2023,19(2): 2089-2098.

[2] Liu S, Li C Q, Hu Q. Cryptanalyzing two image encryption algorithms based on a first-order time-delay system, IEEE Multimedia, 2022, 29(1):74-84.

[3] Hua Z Y, Chen Y Y, Bao H, et al. Two-dimensional parametric polynomial chaotic system, IEEE Transactions on Systems Man Cybernetics-Systems, 2022, 52(7): 4402-4414.

[4] Zhang Y X, Bao H, Hua Z Y, et al. Two-dimensional exponential chaotic system with hardware implementation, IEEE Transactions on Industrial Electronics, 2023, 70(9):9346-9356.

[5] Wang Q Y, Zhang X Q, Zhao X H. Image encryption algorithm based on improved Zigzag transformation and quaternary DNA coding, Journal of Information Security and Applications, 2022, 70:103340.

[6] Gao X Y, Sun B, Cao Y H, et al. A color image encryption algorithm based on hyperchaotic map and DNA mutation, Chinese Physics B, 2023, 32(3):030501.

[7] Liu X L, Tong X J, Wang Z, et al. A novel hyperchaotic encryption algorithm for color image utilizing DNA dynamic encoding and self-adapting permutation, 2022, 81(15):21779-21810.

[8] Gao S, Wu R, Wang X Y, et al. Asynchronous updating Boolean network encryption algorithm, IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(8):4388-4400.

[9] Xian Y J, Wang X Y, Wang X Y, et al. Spiral-transform-based fractal sorting matrix for chaotic image encryption, IEEE Transactions on Circuits and Systems I-Regular Papers, 2022, 69(8):3320-3327.

[10] Nan S X, Feng X F, Wu Y F, et al. Remote sensing image compression and encryption based on block compressive sensing and 2D-LCCCM, Nonlinear Dynamics, 2022, 108(3):2705-2729.

[11] Cai J, Xie S C, Zhang J Z. Image compression-encryption algorithm based on chaos and compressive sensing, Multimedia Toos and Applications, 2023,82(14): 22189-22212.

[12] Liu J L, Zhang M, Tong X J, et al. Image compression and encryption algorithm based on 2D compressive sensing and hyperchaotic system, 2022, 28(2):595-610.

[13] Li L H, Luo Y L, Qiu S H, et al. Image encryption using chaotic map and cellular automata, Multimedia Tools and Applications, 2022, 81(28):40755-40773.

[14] Su Y N, Teng L, Liu P B, et al. Visualized multiple image selection encryption based on log chaos system and multilayer cellular automata saliency detection, IEEE Transactions on Circuits and Systems for Video Technology, 2023, 33(9): 4689-4702.

[15] Zhu C X, Deng X H, Zhang W D, et al. Secure image encryption scheme based on a new robust chaotic map and strong S-box, Mathematics and computers in Simulation, 2023, 207:322-346.

[16] Su Y Y, Tong X J, Zhang M, et al. A new S-box three-layer optimization method and its application, 2023, 111(3):2841-2867.

[17] Hua Z Y, Li J X, Chen Y Y, et al. Design and application of an S-box using complete Latin square, Nonlinear Dynamics, 2021, 104(1):807-825.

[18] Erkan U, Toktas A, Lai Q. 2D hyperchaotic system based on Schaffer function for image encryption, Expert Systems with Applications, 2023, 213:119076.

[19] Toktas A, Erkan U, Ustun D, et al. Parameter optimization of chaotic system using Pareto-based triple objective artificial bee colony algorithm, 2023, 35(18): 13207-13223.

[20] Ye G D, Pan C, Dong Y X, et al. A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition, Transactions on Emerging Telecommunications Technologies, 2021, 32(2): e4071.

[21] Musanna F, Dangwal D, Kumar S, et al. A novel chaos-based approach in conjunction with MR-SVD and pairing function for generating visually meaningful cipher images, Multimedia Tools and Applications, 2020, 79(33-34): 25115-25142.

[22] Yin Z X, Peng Y Y, Xiang Y Z. Reversible data hiding in encrypted images based on pixel prediction and bit-plane compression, IEEE Transactions on Dependable and Secure Computing, 2022, 19(2):992-1002.

[23] An D Z, Hao D W, Zhang S C, et al. Visually semantic-preserving and people-oriented color image encryption based on cross-plane thumbnail preservation, Expert Systems with Applications, 2023,233:120931.

[24] Chai X L, Fu J Y, Gan Z H, et al. An image encryption scheme based on multi-objective optimization and block compressed sensing, Nonlinear Dynamics, 2022, 108(3):2671-2704.

[25] Huang X L, Dong Y X, Ye G D, et al. Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform, Frontiers of Computer Science, 2023, 17(3):173804.

[26] Zhu L Y, Song H S, Zhang X, et al. A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding, Signal Processing, 2020, 175:107629.

[27] Long G Q, Chai X L, Gan Z H, et al. Exploiting one-dimensional Chebyshev chaotic map and matching embedding for visually meaningful image encryption, Chaos Solitons and Fractals, 2023, 176:114111.

[28] Hua Z Y, Zhang K Y, Li Y M, et al. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing, Signal Processing, 2021, 183:107998.

[29] Wang X, Chang C C, Lin C C. Reversible data hiding in encrypted images with block-based adaptive MSB encoding, Information Sciences, 2021, 567:375-394.

[30] Yang Y G, Wang B P, Yang Y L, et al. Visually meaningful image encryption based on universal embedding model, Information Sciences, 2021,562:304-324.

[31] Wu X S, Qiao T, Xu M, et al. Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling, Signal Processing, 2021, 188: 108200.

[32] Yin Z X, Xiang Y Z, Zhang X P. Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding, IEEE Transactions on Multimedia, 2020,22(4):874-884.

[33] Wang Y M, Cai Z C, He W G. High capacity reversible data hiding in encrypted image based on intra-block lossless compression, IEEE Transactions on Multimedia, 2021, 23:1466-1473.

[34] Yang Y, Cheng M, Ding Y Q, et al. A visually meaningful image encryption scheme based on lossless compression SPIHT coding, IEEE Transactions on Services Computing, 2023,16(4):2387-2401.

[35] Sprott A C. Some simple chaotic flows, Physical Review E, 1994, 50(2):647-650.

[36] Cang S J, Li Y, Kang Z J, et al. Generating multicluster conservative chaotic flows from a generalized Sprott-A system, Chaos Solitons and Fractals, 2020, 133:109651.

[37] Cun Q Q, Tong X J, Wang Z, et al. A new chaotic image encryption algorithm based on dynamic DNA coding and RNA computing[J]. Visual Computer, 2023, 39(12):6589-6608.

[38] Bhat J, Moon A H. Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system[J]. Expert Systems with Applications, 2022, 206:117861.

[39] Wang T, Wang M H. Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding[J]. Optics and Laser Technology, 2020, 132: 106355.

[40] Cang S J, Kang Z J, Wang Z H. Pseudo-random number generator based on a generalized conservative Sprott-A system[J]. Nonlinear Dynamics, 2021, 104(1): 827-844.

[41] Jia H Y, Shi W X, Wang L, et al. Energy analysis of Sprott-A system and generation of a new Hamiltonian conservative chaotic system with coexisting hidden attractors[J]. Chaos Solitons & Fractals, 2020, 133:109635.

[42] Qi G Y, Hu J B, Wang Z. Modeling of a Hamiltonian conservative chaotic system and its mechanism routes from periodic to quasiperiodic, chaos and strong chaos[J]. Applied Mathematical Modelling, 2020, 78:350-365.

[43] Jie M, Peng H X, Duan S K, et al. Design and FPGA implementation of grid-scroll Hamiltonian conservative chaotic flows with a line equilibrium[J]. IEEE Transactions on very Large Scale Integration (VLSI) Systems, 2024, 32(4): 658-668.

[44] Candes E J, Romberg J, Tao T. Robust uncertainty principles:: Exact signal reconstruction from highly incomplete frequency information, IEEE Transactions on Information Theory, 2006, 52(2):489-509.

[45] Zhou N R, Li H L, Wang D, et al. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Optics Communications, 2015, 343:10-21.

[46] Zhang B, Xiao D, Xiang Y. Robust coding of encrypted images via 2D compressed sensing, 2021, 23:2656-2671.

[47] Ojala T, Pietikainen M, Harwood D. A comparative study of texture measures with classification based on feature distributions, Pattern Recognition, 1996, 29(1): 51-59.

[48] Wang X Y, Liu C, Jiang D H. An efficient double-image encryption and hiding algorithm using a newly designed chaotic system and parallel compressive sensing, Information Sciences, 2022, 610:300-325.

[49] Yuan Z W, Huang S F, Huang L Q, et al. Safe-LBP: A visually meaningful image encryption scheme based on LBP and compressive sensing, Journal of Information Security and Applications, 2023,78:103591.

[50] Ye G D, Du S M, Huang X L. Image compression-hiding algorithm based on compressive sensing and integer wavelet transformation, Applied Mathematical Modelling, 2023, 124:576-596.

[51] Chai X L, Wu H Y, Gan Z H, et al. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing, Information Sciences, 2021, 556:305-340.

[52] Wang X Y, Liu C, Jiang D H. Visually meaningful image encryption scheme based on new-designed chaotic map and random scrambling diffusion strategy, Chaos Solitons and Fractals, 2022, 164:112625.

[53] Dong Y H, Zhao G, Ma Y J, et al. A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata, Information Sciences, 2022, 593:121-154.

[54] Liu X L, Tong X J, Wang Z, et al. A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its’ applications in image encryption, Chaos Solitons and Fractals, 2022, 154:111693.

[55] Chai X L, Wu H Y, Gan Z H, et al. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding, Optics and Lasers in Engineering, 2020, 124:105837.

[56] Jiang D H, Liu L D, Zhu L Y, et al. Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform, Signal Processing, 2021,188:108220.

[57] Wang X Y, Liu C, Jiang D H. A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding, Expert Systems with Applications, 2023, 209:118426.

[58] Wang X Y, Liu C, Jiang D H. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT, Information Sciences, 2021, 574:505-527.

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

[60] Yang Y G, Wang B P, Pei S K, et al. Using M-ary decomposition and virtual bits for visually meaningful image encryption, Information Sciences, 2021, 580:174-201.

**Declaration of interests**

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.