Image encryption algorithm for crowd data based on a new hyperchaotic system and Bernstein polynomial

Donghua Jiang1 | Lidong Liu1 | Xingyuan Wang2 | Xianwei Rong3

1 School of Information Engineering, Chang’an University, Xian, China
2 School of Information Science and Technology, Dalian Maritime University, Dalian, China
3 Physics and Elecronic Engineering School, Harbin Normal University, Harbin, China

Correspondence
Lidong Liu, School of Information Engineering, Chang’an University, Xian, 710064, China.
Email: liulidong@chd.edu.cn

Funding information
National Key R&D Program of China, Grant/Award Number: 2019YFE0108300; National Natural Science Foundation of China, Grant/Award Numbers: 61701043, 41874140; Shaanxi Province Science and Technology Program, Grant/Award Numbers: 2020JM-220, 2020JQ-351; Fundamental Research Funds for the Central Universities of China, Grant/Award Number: 300102240205

Abstract
A new two-dimensional chaotic system in the form of a cascade structure is designed, which is derived from the Chebyshev system and the infinite collapse system. Performance analysis including trajectory, Lyapunov exponent and approximate entropy indicate that it has a larger chaotic range, better ergodicity and more complex chaotic behaviour than those of advanced two-dimensional chaotic system recently proposed. Moreover, to protect the security of the crowd image data, the newly designed two-dimensional chaotic system is utilized to propose a visually meaningful image cryptosystem combined with singular value decomposition and Bernstein polynomial. First, the plain image is compressed by singular value decomposition, and then encrypted to the noise-like cipher image by scrambling and diffusion algorithm. Later, the steganographic image is obtained by randomly embedding the cipher image into a carrier image in spatial domain through the Bernstein polynomial-based embedding method, thereby realizing the double security of image information and image appearance. Besides, the visual quality of the steganographic image can be improved by the adjustment factor according to different carrier images during the embedding process. Ultimately, security analyses indicate that it has higher encryption efficiency (2 Mbps) and the visual quality of steganography image can reach 39 dB.

1 INTRODUCTION

With the rapid development and large-scale application of communication technologies, more and more digital images are generated and transmitted on public channels. For example, image sensors collect crowd information in real time for understanding and analysis. Because of their sharing and openness, digital images are easy to be acquired illegally or attacked maliciously. How to ensure the security of digital image information has become a hot research topic. Chaotic systems are characterized by pseudo-randomness, long-term unpredictability and high sensitivity to the initial states. Therefore, they are widely used in the design of secure communication systems. Since 1998, Fridrich [1] applied the chaotic system to the digital image encryption for the first time, creating a new era of digital image encryption, the chaotic image encryption algorithms have been developed qualitatively, especially the proposal of new chaotic systems [2–22] and new encryption architectures [23–27].

According to the dimension of the system state space, chaotic systems can be divided into one-dimensional chaotic systems (ODCS) and multi-dimensional chaotic systems (MDSC). With regard to ODCS, due to their simple structure, the resulting chaotic sequences have poor ergodicity, small chaotic range and weak chaotic behaviour, which are easy to be attacked by signal estimation algorithms [28–32]. To address these issues, many improved chaotic system schemes have been proposed. For example, in ref. [2], Cao et al. used an infinite collapse system to modulate the amplitude of another infinite collapse chaotic system with different control parameter to design a novel two-dimensional chaotic system (TDCS). Then the newly designed TDSC was applied to encrypt the plain image for multiple rounds adopted the classic scrambling and diffusion architecture. Hua et al. [5] also proposed an improved scheme to integrate the Logistic map and the Sine map using coupling coefficient, and then extend the integrated ODCS to two dimensions by means of cross iteration. By coupling the two...
ODCS sufficiently, a MDSC with more complex chaotic characteristics can be obtained. Further, the authors used the pseudo-random matrix generated by the newly designed TDCS to scramble and diffuse the plain image for two rounds to obtain the final noise-like cipher image. Besides, Liu et al. designed a new TDCS without modulus operation based on Chebyshev system and Sine system to eliminate the defect of the ODCS in ref. [14], and applied it into the color image encryption. Meanwhile, the initial values of the new chaotic system in ref. [14] are first extracted from the coloured non-Gaussian noise, and then the color cipher image with good avalanche effect can be obtained by using the diffusion matrix to perform exclusive or operation on the components of the plain image. Moreover, in 2020, Liu et al. [3] mentioned a new TDCS with modulo operation, which was obtained by cascading 2D Hénon map and Chebyshev map. During the encryption process, the newly designed TDCS is applied to generate three sets of pseudo-random matrices controlled by the default parameters and the hash value of the plain image, which are used to perform genetic mutation, scrambling and diffusion on the plain image after genetic recombination. Eventually, a cipher image with high security can be obtained. Last but not least, Peng et al. [21] designed a discrete memristor via the difference theory, and applied it to the 2D discrete Hénon map. As far as a chaotic system is concerned, if it has more than two (including two) positive Lyapunov exponents, it indicates that this chaotic system has a more complicated hyperchaotic behaviour. Although the improved chaotic systems mentioned above have very good ergodicity and complex chaotic behaviour, and their chaotic range has also been expanded. The two Lyapunov exponents of the aforementioned 2D chaotic systems are not all greater than zero in the entire parameter interval, so there is still room for improvement in the chaotic performance of these TDCS.

Image encryption technology has been widely used to transmit digital images containing confidential information. However, the cipher images generated by traditional encryption algorithms are texture- or noise-like, which are easily recognized by the human visual system. Therefore, Bao et al. [23] proposed a novel solution of embedding the noise-like cipher image into a visually meaningful carrier image after encryption process, thereby reducing the probability of information leakage and being attacked, and achieving the double security of image information and image appearance. Unfortunately, in Bao’s scheme, the final steganography image is four times the size of the plain image due to the lack of compression, so additional storage space and transmission bandwidth are needed to ensure the security of the plain image information. Besides, ref. [33] also has the same deficiency. In his scheme, the plain image is subjected to pre-processing such as sparse and scrambling, and then the pre-processing image is compressed and quantized using the measurement matrix generated by the logistic-tent chaotic system. In order to improve security and anti-noise performance, random numbers are added to the quantized image before the second scrambling. Finally, the cipher image is hidden in the carrier image by singular value decomposition (SVD) in wavelet domain. To alleviate transmission pressure and save storage space, Chai et al. introduced a set of efficient visually meaningful image encryption scheme in ref. [34]. In Chai’s scheme, before zigzag scrambling the plain image needs to be compressed to a quarter of its original size through compressive sensing technology, and then the cipher image is split and randomly embedded into the carrier image through the least significant bit (LSB) embedding method. Wang et al. [35] also proposed a set of improved visual image encryption algorithm using parallel compressive sensing and embedding technology. Both parallel compressive sensing and zigzag scrambling are applied to generate cipher images in ref. [35]. Additionally, during the embedding process, the embedding order will be disrupted by the index sequence generated by the 3D Cat system to improve the security. Similarly, Wen et al. [36] proposed an improved scheme that uses semi-tensor product compressive sensing to compress the plain image, and then embeds the compressed image after Arnold scrambling into a carrier image through embedding technology, which can not only simultaneously reduce the storage space of the cipher image and the secret keys, but also the quality of the reconstructed image is improved. So far, many excellent visually meaningful image encryption algorithms have been proposed [37–45], but most of them have a common deficiency. That is to say, the identical noise-like cipher image is embedded into different carrier images, and the visual quality of the resulting steganographic images is uneven. If an improper carrier image is selected, the final generated steganographic image will have low visual quality. Meanwhile, the imperceptibility of the cipher image will also be reduced.

For the sake of obtaining a chaotic system with more complex chaotic behaviour, in this paper, a new TDCS with hyperchaotic behaviour based on the Chebyshev system and the infinite collapse system is designed. Moreover, we apply the newly designed TDCS to protect the crowd image data, and propose a meaningful image cryptosystem combined with the SVD and Bernstein polynomial (BP). In proposed scheme, the plain image is compressed to half of its original size by SVD in wavelet domain. Then using the stochastic matrix generated by the newly designed TDCS to scramble and diffuse the compressed image. Finally, the embedding algorithm deduced from the BP is adopted to embed the cipher image into the carrier image randomly. Additionally, the embedding effect is controlled by the adjustment factor, which means that the visual quality of the steganographic image can be adjusted through AF in the light of different carrier images. The contributions of this paper are summarized as follows.

a. A new TDCS with hyperchaotic behaviour over the entire parameter range is designed. Compared with other advanced TDCS proposed in refs. [2–4], performance analysis including system trajectory, Lyapunov exponent and approximate entropy (ApEn) indicate that it has more complex chaotic behaviour and better ergodicity (see Section 3.2).

b. Combining the newly designed TDCS with SVD and BP, a visually meaningful image cryptosystem (VMIC) is proposed. And it does not require additional storage space and transmission bandwidth like refs. [23,33] to improve the visual quality of the steganographic image.
FIGURE 1  Chebyshev system, (a) is the bifurcation chart of the Chebyshev system, (b) is the Lyapunov exponent chart of the Chebyshev system

c. The proposed cryptosystem has high operating efficiency (see section 5.2.6), which can encrypt approximately 2 megabytes of image data per second. Besides, the visual quality of the steganographic images can also be up to 39 dB (see Section 5.2.3).

The remainder of this paper mainly includes following five sections. The second section introduces some indispensable prerequisites. The newly designed 2D chaotic system and performance analysis are mentioned in the third section. Besides, the encryption and decryption process of VMIC are detailedly recorded in the fourth section. And the fifth section is to analyze the security performance of proposed image cryptosystem. The last section will sum up all of our research work.

2  PRELIMINARY KNOWLEDGE

Because of its simple structure and low computational complexity, the ODCS have been widely used in many fields. In this section, two classical ODCS in detail will be introduced, which are Chebyshev system and infinite collapse system. At the same time, the chaotic performance of these two systems is also analyzed.

2.1  Chebyshev system

As one of the classic ODCS, the Chebyshev system with a control parameter $k$ and an initial value $x_0$ is widely used in digital communication [46–48], neural network [49], security issue [50,51] and radio frequency identification [52]. Its mathematical expression is shown in Equation (1). In addition, Equation (2) is expressed as the probability density function of the chaotic sequence generated by Equation (1).

$$x_{n+1} = \cos(k \cos^{-1}(x_n)), \quad x_n \in [-1, 1].$$  \hspace{2cm} (1)

$$\rho(x) = \begin{cases} \frac{1}{\pi \sqrt{1-x^2}} & x \in [-1, 1] \\ 0 & \text{otherwise} \end{cases}.$$  \hspace{2cm} (2)

where $x_n$ represents the discrete state of the output of Chebyshev system, which is located in the interval $[-1, 1]$. The bifurcation chart and Lyapunov exponent chart of the Chebyshev system are shown in Figure 1. It can be seen from Figure 1(a) that under different control parameter conditions, the discrete state of the output of the Chebyshev system presents an uneven distribution. At the same time, when the control parameter $k$ is greater than 1, the Chebyshev system slowly begins to appear bifurcation and enters a chaotic state, which can be verified by the Lyapunov exponent chart in Figure 1(b). Besides, when $k$ is greater than 2, the discrete state of the output is evenly distributed over the entire interval. At this time, the Chebyshev system has very good ergodicity and unpredictability.

2.2  Infinite collapse system

The infinite collapse system, a classical ODS, was firstly proposed by He et al. in 2001 [53], which has the characteristic of infinite collapse times in the interval $[-1, 1]$. Equation (3) represents the mathematical expression of this ODS.

$$x_{n+1} = \sin \left( \frac{a}{x_n} \right), \quad x_n \in [-1, 0) \cup (0, 1].$$  \hspace{2cm} (3)

where $a$ is the control parameter of the infinite collapse system, which belongs to the interval $[0, 4]$. It can be seen from Equation (3) that this system has odd symmetry for the parameter $a$. The bifurcation chart and Lyapunov exponent chart of infinite collapse system are plotted in Figure 2. We can clearly see
from Figure 2 that this chaotic system has non-uniform ergodicity and short chaotic range, which will bring negative effects to its application.

3 | NOVEL 2D CHAOTIC SYSTEM

3.1 | Mathematical definition

As can be seen from the previous section, the chaotic performance and ergodicity of Chebyshev system and infinite collapse system are unevenly distributed, which are easily attacked by the signal estimation algorithm, thereby obtaining the entire trajectory of the chaotic system. For the sake of solving these problems, in this section, we will introduce a new TDCS cascading Chebyshev system and infinite collapse system, which is defined in Equation (4).

\[
\begin{align*}
    x_{n+1} &= \sin\left(\frac{\pi}{2} \cos\left( (4 - \theta) \cos^{-1}\left(x_n\right) \right) \right) \\
    y_{n+1} &= \sin\left(\frac{\pi}{2} \cos\left( (4 - \theta) \cos^{-1}\left(y_n\right) \right) \right) \\
\end{align*}
\]  

In Equation (4), \( \theta \) is the control parameter of the newly designed TDCS in the interval \([0, 4]\). Both \( x_n \) and \( y_n \) represent the discrete states outputted by this chaotic system, which all belong to the interval \([-1, 1]\). It can be seen from the mathematical expression of the newly designed chaotic system that we firstly couple Chebyshev system and infinite collapse system with the parameter \( \theta \). Then the coupled ODCS is extended to two dimensions by means of cross iteration. Finally, map the 2D system to the interval \([-1, 1]\) by Sine function. By combining Chebyshev system with infinite collapse system, not only the key space and chaotic range of the obtained system can be enlarged, but also the chaotic performance can be improved.

3.2 | Performance evaluation

In this subsection, the performance of the newly designed TDCS will be analyzed through system trajectory, Lyapunov exponent, ApEn and National Institute of Standards and Technology (NIST) test. At the same time, in order to demonstrate the superiority, the newly designed TDCS is compared with three advanced TDCS recently proposed by other researchers, The contrasting chaotic systems are the 2D infinite collapse system (referred to as 2D ICS) [2], which is defined in Equation (5), the 2D Hénon-Chebyshev modulation system (referred to as 2D HCMS) [3], which is defined in Equation (6), and the 2D Hénon-Sine system (referred to as 2D HSS) [4], which is defined in Equation (7). Among them, the symbol “mod” denotes the modulo operation.

\[
\begin{align*}
    x_{n+1} &= \sin\left(\frac{a}{y_n} \sin\left(\frac{b}{x_n}\right)\right) \\
    y_{n+1} &= \sin\left(\frac{a}{y_n} \sin\left(\frac{b}{x_n}\right)\right) \\
\end{align*}
\]  

\[
\begin{align*}
    x_{n+1} &= 1 - a \times \cos^2\left(\epsilon \times \cos^{-1}\left(x_n\right) \right) + y_n \mod 1 \\
    y_{n+1} &= b \times x_n \mod 1 \\
\end{align*}
\]  

\[
\begin{align*}
    x_{n+1} &= 1 - a \times \sin^2\left(x_n\right) + y_n \mod 1 \\
    y_{n+1} &= b \times x_n \mod 1 \\
\end{align*}
\]  

3.2.1 | Trajectory analysis

The trajectory chart of a chaotic system is used to analyze the distribution of its attractor in the phase space. As far as a chaotic system is concerned, if its attractor has a complicated geometric distribution and occupies a large area in the phase space, which indicates that this chaotic system has good ergodicity [5]. To visually observe the attractor distribution of the four chaotic systems mentioned above, under the condition that the initial states are all set as \((0.06, 0.03)\), we set the control parameters as 0.62, 1.99 and 2.79 respectively and iterate these chaotic systems 30,000 times. The resulting trajectories are plotted in Figure 3. It can be seen from the figure that (a) when the control parameters are set at 0.62, the attractor distribution of the newly designed
2D chaotic system in this paper is evener than that in refs. [2–4].
(b) Compared with the other three TDCS, the attractors of the proposed 2D chaotic system are also uniformly distributed and occupy almost all the places in the phase space when the control parameters are changed. These indicate that the newly designed chaotic system has good and stable ergodicity.

### 3.2.2 Lyapunov exponent analysis

The Lyapunov exponent (LE) is a significant indicator for quantitatively measuring the characteristics of a dynamical system. It represents the average exponential rate of convergence or divergence between two infinitely close orbitals in the phase space over time. Whether the dynamical system has chaotic behaviour or not can be directly judged by its LE. If its LE is greater than 0, it means that no matter how close the two orbits are in the phase space, the difference would increase exponentially over time to such an extent that it would be unpredictable. The larger the value of its LE is, the more complicated the chaotic behaviour is. In this section, we use the algorithm introduced in ref. [54] to calculate the LE of different 2D chaotic systems. The experimental results are demonstrated in Figure 4. First, compared Figure 4 with Figures 1b and 2b, it can be clearly seen that
the Lyapunov exponent of the TDCS designed in this paper is greater than 0 in the entire parameter interval. That is to say, this newly designed chaotic system has a wider range of chaos than its seed system. Besides, by analyzing Figure 4, we can know that the newly designed chaotic system has a larger Lyapunov exponent compared with other advanced TDCS, such as that in refs. [2–4], and has hyperchaotic characteristics over the entire parameter interval. It further indicates that the newly designed TDCS has superior chaotic behaviour.

3.2.3 Approximate entropy analysis

ApEn, a nonlinear dynamical parameter, is frequently used to qualitatively describe the fluctuation regularity and unpredictability of a time sequence, which was firstly proposed by Pincus [55]. It uses a non-negative number to indicate the complexity and irregularity of a time sequence, reflecting the possibility of new information occurring in the time sequence. The more complex the time sequence is, the higher the ApEn corresponding to it will be. Due to its strong anti-noise performance, easy implementation and low computational demand, we will evaluate the complexity of the above-mentioned 2D chaotic systems through ApEn in this section. Table 1 demonstrates the pseudo-code used to quantitatively calculate the ApEn of a chaotic system. As can be seen from the 12-th row in Table 1, the ApEn actually measures the probability of generating a new pattern in the time sequence when the dimension changes. The greater probability of generating a new pattern, the more complicated the sequence will be, and the greater the corresponding ApEn will be. Therefore, the ApEn can be used to represent the unpredictability and complexity of a time sequence. Through this method, we obtain the approximate entropy curves of four TDCS, as shown in Figure 5. Through the analysis of Figure 5, the time sequence generated by the newly designed TDCS has a higher complexity and unpredictability in the interval [−1,1], compared with the remaining three ApEn curves.

3.2.4 National Institute of Standards and Technology analysis

Pseudo-randomness is one of the inherent characteristics of the chaotic systems. To test the pseudo-randomness of the newly designed TDCS, we will adopt the SP800-22 randomness test suite released by the NIST for experiments. It is widely used to test the randomness of binary sequences generated by secret random or pseudo-random number generators. This test suite uses probability statistics to determine whether the
detected sequence passes each randomness sub-test item or not [56]. Assuming that the significance level \( \alpha \) is 0.01, if the P value generated by the sub-test item is greater than the preset significance level \( \alpha \), then the detected sequence passes this randomness sub-test item. Table 2 below shows the pseudo-code for generating the binary sequence file for testing. We set the initial state as \((0.721, 0.591, 3.47)\) and iterate the newly designed TDCS 1,000,000 times. The final test results are displayed in Table 3 below. It can be seen from the table that the two sets of sequences generated by the newly designed TDCS have passed all sub-item tests, indicating that the chaotic system designed in this paper has good pseudo-randomness.

### Table 2 The pseudo-code of generating a binary sequence for randomness test

| Step | Description |
|------|-------------|
| 1.   | for \( i \) from 1 to \( h w - 1 \) |
| 2.   | \( \chi^{(i+1)} \leftarrow \sin(\pi (4 - \theta (\cos^{-1}(\chi^{(i)})) + \sin(\theta / \chi^{(i)}))) \) |
| 3.   | \( \gamma^{(i+1)} \leftarrow \sin(\pi (4 - \theta (\cos^{-1}(\gamma^{(i)})) + \sin(\theta / \gamma^{(i)}))) \) |
| 4.   | end for |
| 5.   | \( \text{sxq} \leftarrow [\text{sx} \times 10^8] \) |
| 6.   | \( \text{ssi} \leftarrow \text{sxq} \mod 256 \) |
| 7.   | \( \text{sxh} \leftarrow \text{dec2bin(SSI, 8)} \) |
| 8.   | \( \text{fid} \leftarrow \text{ fopen(\text{Txt_Name})} \) |
| 9.   | for \( i \) from 1 to \( \text{length(sxh)} \) |
| 10.  | \( \text{fid} \leftarrow \text{str2double(sxh(i))} \) |
| 11.  | end for |
| 12.  | \( \text{fclose(fid)} \) |

4 | THE PROPOSED VISUALLY MEANINGFUL IMAGE CRYPTOSYSTEM

#### 4.1 Encryption algorithm

The flow chart of the proposed visually meaningful encryption scheme is shown in Figure 6. It can be seen that the encryption scheme mainly consists of compression, encryption and embedding processes. In the compression process, first, perform integer wavelet transform on the plain image to obtain four sub-images \( \text{LL, HL, LH and HH} \). Then the combined image is compressed by SVD, which is obtained by combining the three sub-images \( \text{HL, LH and HH} \). At the same time, a stochastic matrix is also added for filling. Before the encryption process, we need to map the compressed image between \([0, 255]\), and then the pseudo-random matrices generated by the newly designed chaotic system are used to scramble and diffuse the new combined image of the compressed image and the sub-image \( \text{LL} \). In the embedding process, the newly designed TDCS is firstly controlled by secret keys to generate a position index matrix, which is used to determine the embedded position of the cipher image in the carrier image. Secondly, the AF needs to be preset in advance, which is used to control the visual effect of steganographic image. Next, the meaningful image encryption algorithm is described in detail below.

#### 4.1.1 Compression process

Singular value is an important feature of matrix [57]. In numerical analysis, SVD is an algorithm that diagonalizes the matrix, which has many applications in image compression, feature recognition, digital watermarking and other aspects. In this paper, the SVD is utilized to compress the plain image in wavelet domain. Assume that the plain image to be encrypted is \( I \) sized of \( b \times w \). And the image generated in this process is \( \text{JL} \in \mathbb{N}^{b/2 \times w} \).

Step 1: First, perform 2D integer wavelet transform on the plain image \( I \) to obtain four sub-images, namely \( \text{LL} \in \mathbb{N}^{b/2 \times w/2} \), \( \text{HL}, \text{LH} \in \mathbb{N}^{b/2 \times w/2} \), \( \text{HL} \) and \( \text{HH} \) in light of Equation (8). Then perform SVD on the combined image \( \text{CL} \) by Equation (9), in which \( \text{svd(\_)} \) means to perform SVD on the matrix in parentheses, and return the left singular value matrix \( \text{IS} \), the right singular value matrix \( \text{IV} \), and the singular value diagonal matrix \( \text{IV} \).

\[
\text{CL} = [\text{HL, LH, HH}].
\]

\[
[\text{IS, IV, ID}] = \text{svd(CL)}.
\]

Step 2: The combined image \( \text{CL} \in \mathbb{N}^{b/2 \times 3w/2} \) can be obtained by combining the sub-images \( \text{HL, LH and HH} \) in light of Equation (8). Then perform SVD on the combined image \( \text{CL} \) by Equation (9), in which \( \text{svd(\_)} \) means to perform SVD on the matrix in parentheses, and return the left singular value matrix \( \text{IS} \), the right singular value matrix \( \text{IV} \), and the singular value diagonal matrix \( \text{IV} \).

\[
\text{CL} = [\text{HL, LH, HH}].
\]

\[
[\text{IS, IV, ID}] = \text{svd(CL)}.
\]

Step 3: Quantify partial data in matrix \( \text{IS, IV and ID} \). The quantization equation is shown in
| Test items                  | P-value ($x_n$) | Results | P-value ($y_n$) | Results |
|---------------------------|----------------|---------|----------------|---------|
| Frequency test            | 0.419650       | Pass    | 0.992834       | Pass    |
| Block frequency test      | 0.344099       | Pass    | 0.870444       | Pass    |
| Casum-forward test        | 0.263734       | Pass    | 0.373609       | Pass    |
| Casum-reverse test        | 0.238399       | Pass    | 0.379625       | Pass    |
| Runs test                 | 0.243232       | Pass    | 0.607548       | Pass    |
| Longest run test          | 0.808472       | Pass    | 0.480881       | Pass    |
| Rank test                 | 0.669678       | Pass    | 0.801478       | Pass    |
| FFT test                  | 0.524204       | Pass    | 0.433635       | Pass    |
| Non-overlapping template test | 0.595420 | Pass    | 0.424551       | Pass    |
| Overlapping template test | 0.914300       | Pass    | 0.622133       | Pass    |
| Universal test            | 0.167820       | Pass    | 0.225871       | Pass    |
| Approximate entropy test  | 0.988161       | Pass    | 0.841913       | Pass    |
| Random-excursions test ($x = -1$) | 0.259380 | Pass    | 0.570249       | Pass    |
| Random-excursions variant test ($x = 1$) | 0.483932 | Pass    | 0.442645       | Pass    |
| Serial1 test              | 0.164153       | Pass    | 0.774614       | Pass    |
| Serial2 test              | 0.272733       | Pass    | 0.455970       | Pass    |
| Linear complexity test    | 0.862453       | Pass    | 0.361687       | Pass    |

Equation (10)—Equation (12). where the max (·) and min (·) represent the maximum and minimum value of the matrix in parentheses, respectively. ⌊·⌋ indicates rounding to negative infinity.

\[
\text{QIS} = \left[ 255 \times \frac{\text{IS}(\cdot, 1 : k) - \min(\text{IS}(\cdot, 1 : k))}{\max(\text{IS}(\cdot, 1 : k)) - \min(\text{IS}(\cdot, 1 : k))} \right]. \tag{10}
\]

\[
\text{QIV} = \left[ 255 \times \frac{\text{IV}(1 : k, 1 : k) - \min(\text{IV}(1 : k, 1 : k))}{\max(\text{IV}(1 : k, 1 : k)) - \min(\text{IV}(1 : k, 1 : k))} \right]. \tag{11}
\]

\[
\text{QID} = \left[ 255 \times \frac{\text{ID}(\cdot, 1 : k) - \min(\text{ID}(\cdot, 1 : k))}{\max(\text{ID}(\cdot, 1 : k)) - \min(\text{ID}(\cdot, 1 : k))} \right]. \tag{12}
\]

\[
k = \left\lfloor \frac{hw}{2(\theta + 1)} \right\rfloor. \tag{13}
\]

Step 4: Extract the diagonal data in the matrix QIV and denote it as DQIV ∈ $\mathbb{N} \times 1$. The compressed image CPI is then generated on the basis of the combination rule in Figure 7. The purpose of adding a stochastic matrix in the combination process is to make the size of the compressed image exactly $hw/2 \times w/2$. Additionally, because of the compressed image containing stochastic numbers, in this case the cipher images generated by each encryption are different. This plays a certain ability to resist chosen-plaintext attacks.

Step 5: Splice the compressed image CPI and the sub-image LL. The joint equation is shown in Equation (14).

\[
\text{JL} = [\text{LL}, \text{CPI}]. \tag{14}
\]

4.1.2 Encryption process

Since the spliced image JL obtained in the first process has rich contour information, which needs to be encrypted to cover up. The specific encryption operation is shown as follow:

Step 1: Input the first set of secret keys $A: (\theta_0, \Theta_0)$ and iterate the proposed TDCS (Equation (4)) for $(hw/2 + T_0)$ times. $T_0$ is a positive integer greater than 500 to eliminate the negative impacts caused by the transient effect of the chaotic system. Two sets of chaotic sequences $x(0, 0, \theta_0), \ldots, x(0, 0, \theta_0), y(0, 0, \theta_0), \ldots, y(0, 0, \theta_0)$ and $y(0, 0, \Theta_0), \ldots, y(0, 0, \Theta_0)$ for encryption are generated in the end.

Step 2: Sort the chaotic sequences generated in the previous step by Equation (15) to obtain the index sequence, where sort(·) means sort the matrix in parentheses in ascending order and return the corresponding index sequence.

\[
\text{sort}(\cdot), \text{Tx}_c = \text{sort}(\cdot). \tag{15}
\]

Step 3: The scrambled image SCI can be obtained by using index sequence to scramble the spliced image in the column-wise manner. The scrambling equation is shown in Equation (16). Where $i = 1, 2, 3, \ldots, w/2$.

\[
\text{SCI}(i) = \text{JL}(\text{Tx}_c(i)). \tag{16}
\]
Step 4: The final noise-like cipher image $C_I$ can be obtained by using Equation (18) to diffuse the scrambled image.

$$T_{dy} = \text{mod} \left( \text{floor} \left( y \times 10^{10} \right) , 256 \right).$$  \hspace{1cm} (17)

$$C_I = \text{mod} \left( S_{CI} + T_{dy}, 256 \right).$$  \hspace{1cm} (18)

4.1.3 Embedding process

In order for the cipher image to be attacked as little as possible, it is necessary to embed the noise-like cipher image in a visually meaningful carrier image. Therefore, in this sub-section, a novel embedding method based on BP is proposed. BP is widely used in the differential equation and approximate theory [58,59]. Its mathematical model is shown in Equation (19). Since only two images (cipher image and carrier image) are needed in embedding process, $N$ is set to 2. Then the image embedding equation is obtained by simplifying Equation (19), as shown in Equation...
FIGURE 8  The schematic diagram of image embedding

(20), while Equation (21) is the corresponding image extraction equation, where \( f^{(0)} \) and \( f^{(1)} \) represent the meaningless cipher image and the carrier image, respectively. Besides, AF represents the adjustment factor which is used to adjust the hidden visual effect. The schematic diagram of image embedding is demonstrated in Figure 8.

\[
\begin{align*}
\sum_{i=1}^{N-1} \binom{N-1}{i} &\lambda^{N-i-1}(1-\lambda)^{N-1}f^{(0)}, \quad 0 \leq \lambda \leq 1. \quad (19) \\
\lceil Af \times f^{(0)} + (1-Af) \times f^{(1)} \rceil, \quad 0 \leq Af \leq 1. \quad (20) \\
\lceil \frac{(f^{(i)} - (1-Af)f^{(1)})}{Af} \rceil, \quad 0 \leq Af \leq 1. \quad (21)
\end{align*}
\]

Step 1: Input the second set of secret keys B: \((cu_0, cv_0, \theta_1)\) and iterate the newly designed TDSC (Equation (4)) for \(hw + T_0\) times to generate a set of chaotic sequence \(u(u_{T_0+1}, u_{T_0+2}, u_{T_0+3}, \ldots, u_{T_0+T_0})\).

Step 2: Sort the chaotic sequence \(u\) in light of Equation (22) to obtain the corresponding position index sequence.

\[
\lceil, Tcu \rceil = sort(u). \quad (22)
\]

Step 3: Create a blank image \(SI\) and assign all the pixel values of the carrier image \(ZI\) to it. Then the final steganographic image containing cipher information can be obtained through Equation (23), where \(i = 1, 2, 3, \ldots, hw/2\).

\[
SI(Tcu(i)) = \lceil Af \times CI(i) + (1-Af) \times ZI(Tcu(i)) \rceil. \quad (23)
\]

4.2 Decryption algorithm

Similarly, the decryption algorithm also includes three processes, namely extraction, decryption and reconstruction. The detailed decryption steps are as follows.

Step 1: Input the second set of secret keys B: \((cu_0, cv_0, \theta_1)\) and iterate the newly designed TDSC (Equation (4)) to generate the chaotic sequence \(u\). And sort it to obtain the position index matrix \(Tcu\).

Step 2: Extract the cipher image \(CI\) which is hidden in the steganographic image by Equation (24).

\[
CI(i) = \lceil SI(Tcu(i)) - (1-Af) \times ZI(Tcu(i)) \rceil. \quad (24)
\]

Step 3: Utilize the first set of secret keys A: \((cx_0, cy_0, \theta_0)\) to iterate the newly designed TDCS (Equation (4)) to generate the chaotic sequences \(x\) and \(y\). And then the \(Tex\) and \(Tdy\) are obtained by Equation (15) and Equation (17). Later, the inverse scrambling and diffusion operates are executed to obtain the spliced image.
5 | SIMULATION RESULTS AND PERFORMANCE ANALYSIS

5.1 | Simulation results

In this section, simulation experiments will be performed on the proposed VMIC, which are all carried out on a laptop (1.8 GHz i7-8550U CPU and 16G RAM), which is equipped with MITALAB 2018B simulation platform. Six plain images (512 × 512) and six carrier images (512 × 512) are randomly selected for experiments. The secret keys used in the encryption process are set to A: (0.5829, 0.7936, 2.481) and B: (0.9328, −0.5832, 0.9723). In addition, the adjustment factor is set to 0.08. The simulation results demonstrated in Figure 9. It can be clearly seen from the figure that (a) The steganographic images (third column) have a good visualization quality, which are similar to the corresponding carrier images (second column). That is to say the imperceptibility of the cipher image is high. (b) The reconstructed decrypted images (fourth column) obtained by the decryption algorithm are of high quality. Using the BP to embed the cipher image into the carrier image can reduce the probability of illegal acquisition and malicious attacks, which can improve the security of the plain image.

5.2 | Security analysis

5.2.1 | Key space analysis

The key space is a set consisting of all legal initial secret keys during the encryption process. If the key space of the encryption algorithm is too small, the attacker can use the exhaustive attack method to brute force the encryption algorithm. The secret keys of the VMIC proposed in this paper include two parts. The first part of the secret keys is A: (\(c_0, y_0, \theta_0\)), which is used to generate the scrambled sequence and diffused sequence. Another part of the secret keys is B: (\(c_1, y_1, \theta_1\)), which is used to generate the positional index matrix for hiding the noise-like cipher image. Assuming the precision of the floating-point data is 10^{-14}, the total key space is about \(2^{244} \times (10^{14})^2 \times (10^{14})^2 \times (10^{14})^4 \times (10^{14})^2 \times (10^{18})^2 \times (10^{18})^6\), which is larger than that of in refs. [33, 34, 37, 38, 45]. Since its key space is much larger than \(2^{100}\) [60, 61], the image cryptosystem proposed in this paper has enough ability to resist exhaustive attack.

5.2.2 | Key sensitivity analysis

An excellent encryption system not only needs to have a large enough key space to resist exhaustive attacks, but also needs to be sensitive enough to the secret keys. In this subsection, we investigate the sensitivity of the decryption algorithm to the secret keys. Given an infinitesimal change in one of the secret keys and the rest of secret keys remaining unchanged, the corresponding decryption images are shown in Figure 10. It can be seen from the figure that the decrypted images visually do not contain any texture information of the corresponding plain image under the condition of using the wrong secret keys for decryption, even if the secret keys have infinitesimal changes. Next, we use the mean square error (MSE) [62] for further analysis, which is defined in Equation (25).

\[
MSE = \frac{1}{h \times w} \sum_{i=1}^{h} \sum_{j=1}^{w} (P(i, j) - D(i, j))^2.
\]

where \(P\) and \(D\) represent the plain image and the decrypted image respectively. The MSE curves of two sets of secret keys are plotted in Figure 11. The abscissa in Figure 11 represents the added disturbance, and the ordinate represents the MSE between the decrypted image and the plain image. We can clearly see from Figure 11 that whether a small positive or negative disturbance is added to one of the secret keys or not, an erroneous decrypted image is obtained, significantly different from the plain image. It shows that the VMIC is extremely sensitive to the secret keys.

5.2.3 | Histogram analysis

The histogram of natural image depicts the intensity distribution of pixel values. However, as far as the visually meaningful cipher image is concerned, the more similar its histogram is to the corresponding carrier image, the more difficult it is to make statistical analysis on it. Then, the histogram intersection ([35] is adopted to measure the similarity between the meaningful cipher image and the carrier image. Its mathematical model can be calculated from Equation (26).

\[
H(J, V) = \frac{\sum_{i=1}^{256} \min(J_i, V_i)}{\sum_{i=1}^{256} V_i}.
\]

Where \(J\) and \(V\) represent the histograms of the two images, respectively. In the tests, the images Brain and Cameraman, Girl and Barbara, Jet and Baboon are subjected to the proposed meaningful encryption scheme, and the numerical results are listed in Table 4. It can be clearly seen from the table that the distance of histogram intersection of our scheme is higher than that of in refs. [35, 43], indicating that it has a good ability to withstand the statistical attacks.

Step 4: Extract the compressed image CPI from the spliced image. Then perform decomposition, inverse quantization and inverse SVD operations on the compressed image to obtain three sub-images HL, LH and HH.

Step 5: The sub-image LL extracted from the spliced image is stitched with three other sub-images, and then the inverse integer wavelet transform is performed to obtain the recovered plain image I.
FIGURE 9  Simulation results of the proposed algorithm, (a)–(f) are different plain images, (g)–(l) are different carrier images, (m)–(r) are the steganographic images, (s)–(x) are the corresponding decrypted images
FIGURE 10  Experimental results of key sensitivity analysis. (a) Decryption with $c_0 + 10^{-15}$, leaving the rest of the secret keys unchanged. (b) Decryption with $c_0 + 10^{-15}$, leaving the rest of the secret keys unchanged. (c) Decryption with $\theta_0 + 10^{-15}$, leaving the rest of the secret keys unchanged. (d) Decryption with $c_0 + 10^{-15}$, leaving the rest of the secret keys unchanged. (e) Decryption with $c_0 + 10^{-15}$, leaving the rest of the secret keys unchanged. (f) Decryption with $\theta_1 + 10^{-15}$, leaving the rest of the secret keys unchanged.

FIGURE 11  The mean square error curves between the decrypted image and the plain image.

5.2.4  Visualization quality analysis

In this subsection, we evaluate the visual quality of the steganographic image and the imperceptibility of the cipher image, which mainly includes pixel-based evaluation methods and structure-based evaluation methods. Since the peak signal-to-noise ratio (PSNR), a pixel-based evaluation method, can quantitatively measure the distortion introduced by information hiding, which is easy to be calculate. Its mathematical expression is shown in Equation (27) [63], where $\mathbf{D}$ and $\mathbf{I}$ denote the carrier image and the steganographic image, respectively. Additionally, Wang et al. [64] proposed a structure-based distortion evaluation standard, namely the structure similarity in the spatial domain. It expresses the distortion as the three components of structure, brightness and contrast, and then utilizes the total effect formed by these three components to evaluate the quality
The quality of the decrypted image is also an important indicator to judge whether a set of image encryption algorithm is excellent or not. Moreover, the visually meaningful image encryption scheme proposed in this paper has data loss in using SVD to compress the plain image and using BP to hide the corresponding meaningless cipher image. In this subsection, we also adopt the PSNR and MSSIM to measure the difference between the decrypted image and the plain image under different adjustment factors. And the experiment results are shown in Table 7. The table indicates that as the AF increases, the quality of the decrypted image also increases, and the difference from the plain image also gradually decreases. Comparing Table 7 with Table 5, we can find that when the adjustment factor is 0.08, the visual quality of the steganographic images generated during the decryption process is the best, and the decrypted images generated during the decryption process also has a high quality. The biggest advantage of this VMIC is that users can weigh the relationship between the visual quality of steganographic image and the quality of reconstructed image, and set appropriate AF to apply to different carrier images.

Next, we will compare the quality of the decrypted images in different meaningful image encryption algorithms. In the comparative experiment, the compression rates in refs. [33, 34, 37, 45] are set to 0.25, and the AF in this paper is set to 0.08. The experimental results are demonstrated in Table 8. As can be seen from the table, the quality of the decrypted images produced by the proposed VMIC is better than that of other algorithms in refs. [33, 34, 37, 45]. Besides, if a higher quality decrypted image is required, the AF can be increased appropriately.

5.2.6 | Noise and cropping attack analysis

Images are often affected by noise during transmission on public networks, causing different degrees of image distortion. In order to investigate the anti-noise and anti-cropping performance of the VMIC proposed in this paper, the steganographic images are cut in different specifications, and different strengths of pepper and salt noise (SPN) are added in the experiment. The experimental results are demonstrated in Tables 9 and 10. It can be seen from the two tables that, with the increase of attack intensity, the texture information of the decrypted image becomes more and more blurred, but the contour information contained in the decrypted image can still be clearly seen, indicating that the algorithm presented in this paper has good anti-noise and anti-cropping properties. In addition, it has the same ability to resist noise and cropping attacks under different adjustment factors.

5.2.7 | Running efficiency analysis

Operational efficiency is also an indispensable indicator for measuring the overall performance of an encryption algorithm. Figure 12 shows the time required to encrypt a Lena image with the size of 512 × 512 and the percentage consumed by each part of the encryption algorithm. It can be seen from the Figure 12 that the hiding process takes the longest time, accounting for about 60% of the total time. Besides, the compression process also occupies a considerable percentage of an image. And Equation (28) is the mathematical expression for calculating the mean structural similarity (MSSIM). Where \( \mu_D \) and \( \sigma_D \) represent the mean and standard deviation of the \( i \)-th non-overlapping sub-block in the image \( D \), respectively.

\[
\text{PSNR} = 10 \times \log \left( \frac{1}{L \times \sum_{i=1}^{L} \sum_{j=1}^{L} (D(i, j) - I(i, j))^2} \right) \quad \quad (27)
\]

\[
\text{MSSIM} = \frac{1}{L} \times \sum_{i=1}^{L} \left( \frac{2\mu_D \mu_I + (0.01 \times 255)^2}{(\mu_D^2 + \mu_I^2 + (0.01 \times 255)^2) \times \frac{2\sigma_D \sigma_I + (0.03 \times 255)}{(\sigma_D^2 + \sigma_I^2 + (0.03 \times 255))^2}} \times \frac{\sigma_D^2 + \frac{1}{2} (0.03 \times 255)^2}{\sigma_D^2} \right) \quad \quad (28)
\]

We select two groups of images (Lena and Woman, Boat and Peppers) for the experiments under different adjustment factors. And the experimental results are displayed in Table 5. It can be clearly seen from the table that the AF decreases, the visual quality of the steganographic images and the imperceptibility of the cipher images get better and better. Especially when the adjustment factor AF is 0.04, the PSNR and MSSIM of the steganographic images are about 39 dB and 98%, respectively, indicating that the steganographic images have a high similarity with the corresponding carrier images. Besides, when AF = 0.08, the comparison results of the visual quality for multiple meaningful image encryption algorithms are listed in Table 6. As described in the table, the cipher image provided by the proposed meaningful image encryption has better imperceptibility compared with the refs. [33, 37, 45]. However, ref. [34] embeds the meaningless cipher image into a carrier image via the LSB embedding method, which can reduce the damage intensity to the pixel of the carrier image. Therefore, the visual quality of the proposed scheme is inferior to that of ref. [34].
### Table 5: Experimental results of visual quality analysis

| Condition | Plain image | Carrier image | Stego image | Result               |
|-----------|-------------|---------------|-------------|---------------------|
| AF = 0.10 | ![Plain image](image1) | ![Carrier image](image2) | ![Stego image](image3) | PSNR = 31.26502 \(\text{MSSIM} = 0.91651\) |
| AF = 0.08 | ![Plain image](image5) | ![Carrier image](image6) | ![Stego image](image7) | PSNR = 33.24746 \(\text{MSSIM} = 0.94481\) |
| AF = 0.04 | ![Plain image](image10) | ![Carrier image](image11) | ![Stego image](image12) | PSNR = 39.23870 \(\text{MSSIM} = 0.98531\) |
| AF = 0.10 | ![Plain image](image15) | ![Carrier image](image16) | ![Stego image](image17) | PSNR = 30.96448 \(\text{MSSIM} = 0.91574\) |
| AF = 0.08 | ![Plain image](image20) | ![Carrier image](image21) | ![Stego image](image22) | PSNR = 33.00281 \(\text{MSSIM} = 0.94475\) |
| AF = 0.04 | ![Plain image](image25) | ![Carrier image](image26) | ![Stego image](image27) | PSNR = 38.97481 \(\text{MSSIM} = 0.98510\) |

### Table 6: Comparison of the visual quality with other algorithms

| Plain image | Carrier image | Algorithm | PSNR (dB) |
|-------------|---------------|-----------|-----------|
| Lena.bmp (512×512) | Peppers.bmp (512×512) | Proposed | 33.25    |
|              |               | Ref. [45] | 31.47    |
|              |               | Ref. [33] | 32.95    |
|              |               | Ref. [34] | 36.59    |
|              |               | Ref. [37] | 30.28    |

Next, the efficiency is compared with other different encryption schemes, and the experimental results are demonstrated in Table 11. As can be clearly seen from the table, the operating efficiency of the VMIC is significantly better than that of in the refs. [33, 34, 37, 38]. The proposed encryption algorithm mainly in this paper involves the following three operations: floating-point arithmetic, floating-point sorting and integer exchange. As far as refs. [33, 34, 37] are concerned, the compressive sensing technology that is used
TABLE 7  Experimental results of reconstruction quality analysis

| Condition | Plain image | Stego image | Decrypted image | Result                    |
|-----------|-------------|-------------|-----------------|---------------------------|
| AF = 0.10 |             |             |                 | PSNR = 33.99900          |
|           |             |             |                 | MSSIM = 0.94977           |
| AF = 0.08 |             |             |                 | PSNR = 33.18483           |
|           |             |             |                 | MSSIM = 0.92502           |
| AF = 0.04 |             |             |                 | PSNR = 28.82948           |
|           |             |             |                 | MSSIM = 0.78361           |
| AF = 0.10 |             |             |                 | PSNR = 31.71434           |
|           |             |             |                 | MSSIM = 0.96133           |
| AF = 0.08 |             |             |                 | PSNR = 30.61178           |
|           |             |             |                 | MSSIM = 0.94147           |
| AF = 0.04 |             |             |                 | PSNR = 26.74384           |
|           |             |             |                 | MSSIM = 0.82154           |

TABLE 8  Comparison of the image reconstruction quality with other algorithms

| Plain image | Carrier image | Algorithm | PSNR (dB) |
|-------------|---------------|-----------|-----------|
| Lena.bmp (512 × 512) | Peppers.bmp (512 × 512) | Proposed | 33.18 |
|              |               | Ref. [45] | 32.62 |
|              |               | Ref. [33] | 32.98 |
|              |               | Ref. [34] | 33.06 |
|              |               | Ref. [37] | 28.54 |

To compress the plain images in the encryption process requires a series of processes such as plain image sparsification, measurement matrix construction and sparse image compression, which are time-consuming compared with the three operations mentioned above.

6  CONCLUSION

In this paper, a new TDCS with hyperchaotic behaviour over the entire parameter range is designed by cascading the
TABLE 9  The first group of robustness test results

| Condition                  | Plain image | Stego image | Decrypted image | Result                      |
|---------------------------|-------------|-------------|-----------------|----------------------------|
| AF = 0.1 cropping attack  |             |             |                 | PSNR = 21.773              |
| (Intensity: 0.125)        |             |             |                 | SSIM = 0.5023              |
| AF = 0.1 cropping attack  |             |             |                 | PSNR = 14.924              |
| (Intensity: 0.25)         |             |             |                 | SSIM = 0.1659              |
| AF = 0.1 Noise attack     |             |             |                 | PSNR = 16.226              |
| (Intensity: 0.05 SPN)     |             |             |                 | SSIM = 0.2056              |
| AF = 0.1 Noise attack     |             |             |                 | PSNR = 12.529              |
| (Intensity: 0.1 SPN)      |             |             |                 | SSIM = 0.0993              |

FIGURE 12  Total encryption time and time consumption percentage of each part in the proposed algorithm for Lena (512 × 512)

Chebyshev system and the infinite collapse system to solve the shortcomings of ODCS applied in secure communication. The performance analyses indicate that compared with other current existing advanced TDCS, the newly designed TDCS has more complex chaotic behaviour and better ergodicity. Besides, the key space and chaos range are all expanded. Then the newly designed chaotic system is utilized to protect the crowd data, and a novel visually meaningful image encryption algorithm is proposed, which consists of compression, encryption and embedding. Finally, simulation results and security performance
analyses demonstrate that the proposed visually meaningful image crypto-system has good visual security, decryption quality and robustness, indicating that it has a wide range of application scenarios. In the following work, we will aim to further improve the efficiency of information transfer by hiding multiple cipher images into a carrier image using the fractional Fourier transform-based embedding method.

ACKNOWLEDGEMENTS
The authors are grateful to editors and the anonymous reviewers for their valuable suggestions to improve the quality of this paper. Simultaneously, the authors are also grateful to Prof. Hua Zhongyun for his guidance on this paper in the early stage. Last but no least, this work was supported by the National Key R&D Program of China (Grant No. 2019YFE0108300), the National Natural Science Foundation of China (Grant No. 61701043, 41874140), the Shaanxi Province Science and Technology Program (Grant No. 2020JM-220, 2020JQ-351), the Fundamental Research Funds for the Central Universities of China (Grant No. 300102240205).

ORCID
Donghua Jiang https://orcid.org/0000-0002-3545-6409
Lidong Liu https://orcid.org/0000-0001-8142-2261

REFERENCES
1. Fridrich J.: Symmetric ciphers based on two-dimensional chaotic maps. Int. J. Bifurcation Chaos. 08(6), 1259–1284 (1998)
2. Cao W., Mao Y., Zhou Y.: Designing a 2D infinite collapse map for image encryption. Signal Process 171, 107457, (2020)
3. Liu Y., et al.: A chaotic image encryption scheme based on Hénon-Chelyshev modulation map and genetic opere- rations. Int. J. Bifurcation Chaos. 30(6), 2050090 (2020)
4. Wu J., Liao X., Yang B.: Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process. 153, 11–23 (2018).

5. Hua Z., et al.: 2D logistic-sine-coupling map for image encryption. Signal Process. 149, 148–161 (2018).

6. Wang J., et al.: A novel chaotic system and its application in a color image cryptosystem. Opt. Lasers Eng. 121, 479–494 (2019).

7. Hua Z., Zhou Y.: Image encryption using 2D Logistic-adjusted-Sine map. Inf. Sci. 339, 237–253 (2016).

8. Wang X., Li Y., Jin J.: A new one-dimensional chaotic system with applications in image encryption. Chaos Solitons & Fractals 139 110102 (2020).

9. Pak C., Huang L.: A new color image encryption using combination of the 1D chaotic map. Signal Process. 138, 129–137 (2017).

10. Awalida M., et al.: A new hybrid digital chaotic system with applications in image encryption. Signal Process 160, 45–58 (2019).

11. Wang X., et al.: High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices. Opt. Lasers Eng. 122, 225–238 (2019).

12. Hua Z., et al.: 2D sine logistic modulation map for image encryption. Inf. Sci. 297, 80–94 (2015).

13. Diab H.: An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. IEEE access 6, 42227–42244 (2018).

14. Liu S., Wu F., Kadir A.: Construction of a new 2D Chebyshev-Sine map and its application to color image encryption. Multimedia Tools Appl. 78(12), 15997–16010 (2019).

15. Kang X., et al.: Homogenized Chebyshev-Arnold map and its application to color image encryption. IEEE access 7, 114459–114471 (2019).

16. Wang N., et al.: Generating multi-scroll Chaotic attractors via simplified Piecewise-linear Chua’s diode. IEEE Trans. Circuits Syst. I-Regul. Pap. 66(12), 4767–4779 (2019).

17. Hua Z., et al.: Designing hyperchaotic Cat maps with any desired number of positive Lyapunov exponents. IEEE T. Cybern. 48(2), 463–473 (2018).

18. Kapitanak T., et al.: A new chaotic system with stable equilib-rium: Entropy analysis, parameter estimation, and circuit design. Entropy. 20(9), 670 (2018).

19. Wu G., et al.: New variable-order fractional chaotic systems for fast image encryption. Chaos. 29(8), 083103 (2019).

20. Tian Y., Lu Z.: Chaotic S-box: Six-dimensional fractional Lorenz-Duffing chaotic system and O-shaped path scrambling. Nonlinear Dyn. 94, 2115–2126 (2018).

21. Peng Y., Sun K., He S.: A discrete memristor model and its application in Hénon map. Chaos Solitons & Fractals. 137, 109873 (2020).

22. Peng Y., He S., Sun K.: A higher dimensional chaotic map with discrete memristor. Int. J. Electron. Commun. (AEÜ). 129, 155339 (2021).

23. Bao L., Zhou Y.: Image encryption: Generating visually meaningful encrypted images. Inf. Sci. 324, 197–207 (2015).

24. Liu S., et al.: A plaintext-related dynamical image encryption algorithm based on permutation-combination-diffusion architecture. IEEE access 8, 62785–62799 (2020).

25. Ye G., et al.: A chaotic image encryption algorithm based on information entropy. Int. J. Bifurcation Chaos. 28(1), 1850010 (2018).

26. Huang H., et al.: A compression-diffusion permutation strategy for securing image. Signal Process 150, 183–190 (2018).

27. Liu S., Lei Y., Wang D.: A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation. IEEE access 8, 27361–27374 (2020).

28. Ponura R., Anutha R.: Compressive sensing based image compression-encryption using novel 1D chaotic map. Multimed. Tools Appl. 77(15), 19209–19234 (2018).

29. Huan L., Bo R.: The estimation of chaotic signal initial value. in: International Conference on Measuring Technology and Mechatronics Automation. 540–543 (2009). doi:10.1109/ICMTMA.2009.419.

30. Wu X., Hu H., Zhang B.: Parameter estimation only from the symbolic sequences generated by chaos system. Chaos Solitons Fractals 22(2), 359–366 (2004).

31. Li C., et al.: Cryptanalyzing an image encryption algorithm based on auto-heading and electrocardiography. IEEE Multimedia 25(4), 46–56 (2018).

32. Kurian A., Leung H.: Weak signal estimation in chaotic clutter using model-based coupled synchronization. IEEE Trans. Circuits Syst. I-Regul. Pap. 56(4), 820–828 (2009).

33. Ye G., et al.: Image encryption and hiding algorithm based on compressive sensing and random numbers insertion. Signal Process 172, 107563 (2020).

34. Chai X., et al.: An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. Opt. Lasers Eng. 124, 105837 (2020).

35. Wang H., et al.: A visually secure image encryption scheme based on parallel compressive sensing. Signal Process 155, 218–232 (2019).

36. Wen W., et al.: A visually secure image encryption scheme based on semi-tensor product compressed sensing. Signal Process 173, 107580 (2020).

37. Chai X., et al.: A visually secure image encryption scheme based on compressive sensing. Signal Process 134, 35–51 (2017).

38. Kanso A., Ghaleb M.: An algorithm for encryption of secret images into meaningful images. Opt. Lasers Eng. 90, 196–208 (2017).

39. Thanki R., et al.: A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory. Imaging Sci. J. 65(8), 457–467 (2017).

40. Xu Q., Sun K., Zhu C.: A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map. Phys. Scr. 95(3), 035223 (2020).

41. Armijo-Correa J., et al.: An improved visually meanin-gful encrypted image scheme. Opt. Laser Technol. 127, 106165 (2020).

42. Ping P., et al.: Meaningful encryption: Generating visually meaningful encrypted images by compressive sensing and reversible color transformation. IEEE access 7, 170168–170184 (2019).

43. Ponura R., et al.: Visually meaningful image encryption using data hiding and chaotic compressive sen- sing. Multimed. Tools Appl. 78(18), 25707–25729 (2019).

44. Singh L., Singh K.: Visually meaningful multi-image encryption scheme, Arab. J. Sci. Eng. 43(12), 7397–7407 (2018).

45. Zhu L., et al.: A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding. Signal Process 175, 107629 (2020).

46. Luo X., et al.: A new image encryption algorithm using homoge-nized Chebyshev-Arnold map. in: Proceedings of 2018 14th IEEE International conference on signal processing (ICSP). 317–322 (2018). doi:10.1109/ICSP2018.8652390.

47. Javeed A., Shah T.: Cryptosystem techniques based on the improved Chebyshev map: An application in image encryption. Multimedia. Tools Appl. 78(22), 31467–31484 (2019).

48. Yan S., Xiao Z.: Application of BP neural network with Chebyshev mapping in image compression. in: The 3rd International Conference on Instrumentation Measurement Computer Communication and Control (IMCCC). 398–402 (2013). doi:10.1109/IMCCC.2013.91.

49. Akritas P., Antoniou I., Ivanov V.: Identification and prediction of discrete chaotic maps applying a Chebyshev neural network. Chaos Solitons Fractals. 11(1–3), 337–344 (2000).

50. Wang X., et al.: A new key agreement protocol based on Chebyshev chaotic maps. Secur. Commun. Netw. 9(18), 5028–5035 (2016).

51. Chatterjee S., et al.: Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment. IEEE Trans. Dependable Secur. Comput. 15(5), 824–839 (2018).

52. Zhang Z., Wang H., Gao Y.: C2MP: Chebyshev chaotic map-based authentication protocol for RFID applications. Pers. Ubiquitous Comput. 19(7), 1053–1061 (2015).

53. He D., et al.: Chaotic characteristics of a one-dimensional iterative map with infinite collapse. Proceedings of 2018 IEEE International conference on wireless communications and signal processing (WCSP). 2018.

54. Briggs K.: An improved method for estimating Liapunov exponents of chaotic time series. Phys. Lett. A. 151(1–2), 27–32 (1990).

55. Pincus S.: Approximate entropy as a measure of system complexity. Proc. Natl. Acad. Sci. USA. 88, 2297–2301 (1991).

56. Iwasaki A.: Analysis of NIST SP800-22 focusing on randomness of each sequence. JSIAM Letters 10, 1–4 (2018).

57. Stewart G.: On the early history of the singular value decomposition. SIAM Rev 35(4), 551–566 (1993).
58. Selvalakshmi V., Devi S.: A novel region based segmentation of hepatic tumors and hepatic vein in low contrast CTA images using Bernstein polynomials. Biomed. Res. 28, S324–S331 (2017)

59. Ramya M., Krishnaveni V., Sridharan K.: Certain investigation on iris image recognition using hybrid approach of Fourier transform and Bernstein polynomials. Pattern Recognit. Lett. 94, 154–162 (2017)

60. Xu Q., et al.: An effective image encryption algorithm based on compressive sensing and 2D-SLIM. Opt. Lasers Eng. 134, 106178 (2020)

61. Kaur M., et al.: Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map. Future Gener. Comp. Sy. 107, 333–350 (2020)

62. Liu L., et al.: A dynamic triple-image encryption scheme based on chaos, S-box and image compressing. IEEE Access 8, 210382–210399 (2020)

63. Liu L., Zhang Z., Chen R.: Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos. IEEE Access 7, 126450–126463 (2019)

64. Zhou W., et al.: Image quality assessment: From error visibility to structural similarity. IEEE Trans. Image Process. 13(4), 600–612 (2004)

How to cite this article: Jiang D., et al.: Image encryption algorithm for crowd data based on a new hyperchaotic system and Bernstein polynomial. IET Image Process. 1–20 (2021).
https://doi.org/10.1049/ipr2.12237