Signal Processing 195 (2022) 108489

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing

Liya Zhu[a], Donghua Jiang[b,*], Jiangqun Ni[c], Xingyuan Wang[d], Xianwei Rong[e], Musheer Ahmad[f], Yingpin Chen[g]

[a] School of Electronics and Control Engineering, Chang'an University, Xi'an 710064, China
[b] School of Information Engineering, Chang'an University, Xi'an 710064, China
[c] School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 511400, China
[d] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[e] Physics and Electronic Engineering School, Harbin Normal University, Harbin 150025, China
[f] Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[g] School of Physics and Information Engineering, Minnan Normal University, Zhangzhou 363000, China

ARTICLE INFO

Article history:
Received 19 November 2021
Revised 22 January 2022
Accepted 27 January 2022
Available online 29 January 2022

Keywords:
Image security
Visually meaningful cipher image
Chaotic map
Compressive sensing
Discrete V transform

ABSTRACT

In order to safely and covertly protect the digital image information during public channel transmission and localized storage, a stable image visually secure encryption algorithm by using 2D discrete fractional-order chaotic map (FOCM), Bayesian compressive sensing (BCS), and discrete V transform (DVT) is presented in this paper. First, the key-controlled measurement matrix constructed by the infinite collapse-Chebyshev-coupling chaotic map is employed to measure the scrambled wavelet packet coefficients of plain image in parallel. Then, the fractional-order chaotic map designed through piece-wise constant arguments method is employed to generate the secret code streams with assistance of the counter mode, and under its control, the compressed image is re-encrypted into the intermediate secret image. Next, the DVT-based embedding technology is proposed to stochastically embed the secret data into the non-secret-involved host image. Eventually, experimental results show that under the premise of ensuring security, the proposed algorithm improves the visual security around 1∼9 dB, and stabilizes its compression performance within 1 dB, compared with other existing related encryption algorithms.

1. Introduction

With the evolution of multimedia technology and the popularization of mobile Internet, digital images have been widely utilized as the significant digitized carrier for storing and transmitting information in various fields. However, in the open network environments, the potential security risks confronted by digital image cannot be underestimated, such as monitoring, tampering, embezzlement and destruction. To protect image security effectively, image encryption technology is of great research value, as well as has become a hot research issue in the information security field.

The unpredictable irregular movement of chaotic systems and their extreme sensitivity to the initial states make them develop rapidly in the secure communication field [1,2]. Up to now, a variety of high-security and visually meaningless image encryption schemes have been proposed by combining chaos theory with other technologies, such as neural network [3,4], quantum technology [5,6], tensor theory [7], compressive sensing [8–10] and cellular automata [11]. Besides, as the research moves along, some researchers are targeted to analyze the features of different types of images including remote sensing image, thumbnail image, and medical image, and then put forward the corresponding encryption schemes [12–14]. Nevertheless, there exist some defects in the image encryption schemes discussed above. The first point is that in the most of encryption schemes, high-dimensional chaotic systems are adopted to improve security performance. But meanwhile, the computational overhead is too high for the practical application. Next, the second point is that the cipher image is noise-like and visually meaningless, which could make it easy to be detected by hackers, enhancing the probability of being attacked.

In order to protect the data and appearance of image synchronously, the authors in Ref.[15] introduced a visually secure encryption framework, that is, the noise-like encrypted image produced by the encryption methods is embedded into a certain

* Corresponding author.
E-mail address: jiangdonghua@chd.edu.cn (D. Jiang).

https://doi.org/10.1016/j.sigpro.2022.108489
0165-1684/

host image through the lifting wavelet transform. Similarly with Ref.[16], due to the lack of compression layer, additional storage and transmission costs are increased. Subsequently, the compressive sensing technology is exploited and introduced into the design of visually secure encryption algorithm by Chai et al. [17,18] to curtail the unnecessary resources. However, as pointed out in Ref.[19], the essence of CS-based compression is a linear projection, so it cannot defend against the plaintext attacks (PA). Then, the strategy of updating the secret keys through the hash value of the plaintext [20,21] or counter mode [22,23] is developed to improve the capacity of withstanding the plaintext attacks. In other aspects, as far as the existing visually secure encryption schemes based on the spatial-domain embedding are concerned, such as the least significant bit [24], pixel value differencing [25] and histogram shifting [26], it is difficult for them to balance their imperceptibility with robustness and embedding capacity.

In this paper, we exploit a stable visually meaningful image encryption scheme using the newly designed 2D discrete fractional-order chaotic map, the Bayesian compressive sensing and the DVT-based embedding approach. And the presented encryption scheme is composed of two prime stages. First, in the encryption stage, before utilizing Bayesian CS to compress a certain plain image to acquire the non-semantic secret image, the 2D Arnold scrambling, which is easy to be implemented and can gain good scrambling effect, is employed to scramble the plaintext sparse coefficients. Then in the embedding phase, the secret image is stochastically embedded into the publicly accessible host image in frequency domain using the DVT embedding to produce the meaningful cipher image without expanding the dimension. Additionally, with the assist of plaintext eigenvalue and counter mode, the proposed fractional-order chaotic map is employed to produce the updated secret code streams for the encryption scheme.

Our contributions and innovations are given as follows:

(1) To improve the unpredictability and complexity of secret code streams, a lightweight two-dimensional fractional-order discrete chaotic map is designed.
(2) To visually encrypt the noise-like secret image, degrading the probability of being attacked, a lossy embedding approach based on DVT is developed.
(3) To successfully defend against the CPA and KPA, a dynamic secret keys update mechanism combining plaintext eigenvalue with counter mode is proposed.
(4) In terms of new fractional-order chaotic map, Bayesian compressive sensing and DVT embedding, a new image encryption scheme to create visually secure cipher image is presented. Moreover, it is worth mentioning that compared with traditional CS, Bayesian CS can increase the reliability of signal reconstruction and stabilize the compressibility of the proposed scheme.

The rest of this article consists of the following sections. Section 2 briefly introduces some fundamental knowledge including fractional calculus, Bayesian compressive sensing and discrete V transform. Section 3 presents the newly designed discrete fractional-order chaotic map and its performance analysis. Then, Section 4 detailedly depicted the implementation steps of proposed meaningful image encryption scheme and its decryption steps. Later, Section 5 and Section 6 respectively give the results of simulation experiment, performance analysis and comparison. Finally, the last section summarizes our work.

2. Fundamental knowledge

2.1. Discrete fractional calculus

As the extension of integer-order calculus, the fractional calculus has been widely adopted in the past decades and has acquired fruitful results [27]. But meanwhile, one of its drawbacks is that the computational complexity is higher than the integer-order calculus operation. Therefore, the discretization theory of fractional calculus operators has been developed rapidly. In this paper, one of our works is to extend the newly designed two-dimensional continuous chaotic system to fractional-order system, and then discretize it for generating a two-dimensional discrete chaotic system with low complexity and excellent chaotic characteristics. The following are the concepts related to discrete fractional calculus.

For the factorial polynomial

$$t^{(n)} = \prod_{j=0}^{n-1}(t-j) = \frac{\Gamma(t+1)}{\Gamma(t+1-n)} \tag{1}$$

where the symbol $\Gamma(t+1)$ is the Gamma function. If there is $t+1-j=0$ for some j value, then the output value of Eq. (1) is appointed to be zero. To extension of n, the following equation is defined.

$$t^{(v)} = \frac{\Gamma(t+1)}{\Gamma(t+1-v)}, \quad v>0 \tag{2}$$

Iteratively define the operator $\Delta^j = \Delta(\Delta^{j-1})$, where j is a non-negative integer. Δ^0 is the constant operator and $\Delta^1 f(t) = \Delta f(t) = f(t+1) - f(t)$. Let $N_a = \{a, a+1, ...\}$ represents the discrete time scale, where the $a \in \mathbb{R}$ is fixed. For the initial value problem of the following equation

$$\begin{cases} \Delta^n u(t) = f(t), & t \in N_a \\ u(a+j-1) = 0, & j = 1, 2, ..., n \end{cases} \tag{3}$$

its solution is

$$\Delta^{-n} f(t) = u(t) = \sum_{s=a}^{t-1} \frac{(t-\sigma(s))^{(n-1)}}{(n-1)!} f(s) \tag{4}$$

where $\sigma(s) = s+1$. Besides, when $s = t-(n-1), ..., t-1$, $(t-\sigma(s))^{(n-1)}/(n-1)! = 0$, and then

$$\begin{aligned} \sum_{s=a}^{t-1} \frac{(t-\sigma(s))^{(n-1)}}{(n-1)!} f(s) &= \sum_{s=a}^{t-n} \frac{(t-\sigma(s))^{(n-1)}}{(n-1)!} f(s) \\ &= \frac{1}{(n-1)!} \sum_{s=a}^{t-n} \frac{\Gamma(t-s)}{\Gamma(t-s-(n-1))} f(s) \end{aligned} \tag{5}$$

Therefore, there is the following definition.

Definition 1. [28] Suppose $v>0$ and $\sigma(s) = s+1$, then

$$\Delta^{-v} f(t) = \frac{1}{\Gamma(v)} \sum_{s=a}^{t-v} \frac{\Gamma(t-s)}{\Gamma(t-s-(v-1))} f(s), \quad v>0 \tag{6}$$

where $\Delta^{-v} f(t)$ is called as the v-order fractional sum of the function f. Attentively, Δ^{-v} has mapped the function defined on N_a to N_{a+v}.

According to **Definition 1**, the v-order Caputo fractional difference of the function f can be defined as follows.

Definition 2. [28] Let $v>0, v \notin \mathbb{N}$, define

$$\begin{aligned} {}^C\Delta_a^v f(t) &= \Delta^{-(n-v)} \Delta^n f(t) \\ &= \frac{1}{\Gamma(n-v)} \sum_{s=a}^{t-(n-v)} (t-\sigma(s))^{(n-v-1)} \Delta_s^n f(s) \end{aligned} \tag{7}$$

as the v-order fractional difference of the function f, where $n = [v]+1$. Additionally, if $v = n = \mathbb{N}^*$, then ${}^C\Delta_a^v f(t) = \Delta^n f(t)$.

Lemma 1. [29] For the Caputo fractional difference equation

$$\begin{cases} {}^C\Delta_a^v u(t) = f(t+v-1, u(t+v-1)) \\ \Delta^k u(a) = u_k, n = [v]+1, k = 0, 1, ..., n-1 \end{cases} \tag{8}$$

its equivalent equation is

$$u(t) = u_0(t) + \frac{1}{\Gamma(\nu)} \sum_{s=a+n-\nu}^{t-\nu} (t - \sigma(s))^{(\nu-1)} f(s+\nu-1, u(s+\nu-1)),$$
$$t \in \mathbb{N}_{a+n} \tag{9}$$

where

$$u_0(t) = \sum_{k=0}^{n-1} \frac{(t-a)^{(k)}}{k!} u_k.$$

2.2. Bayesian compressive sensing

The basic model of compressive sensing [30] can be described as

$$Y = \Phi X + v \tag{10}$$

where $Y \in \mathbb{R}$ sized of $M \times 1$ is the compressed signal, $\Phi \in \mathbb{R}$ sized of $M \times N$ is the perception matrix and $X \in \mathbb{R}$ sized of $N \times 1$ is the natural signal. Besides, v is the Gaussian white noise (WGN) following the distribution $N(0, \sigma_0^2)$.

Generally speaking, the natural signal X is not sparse, that is, most of its elements are non-zero. Thus, the dictionary matrix D is usually adopted to realize the sparseness of signal, which can be expressed by Eq. (11).

$$X = DW \tag{11}$$

where W is the coefficient matrix of signal X on the dictionary $D = [d_1, d_2, ..., d_i]$, and it is sparse. Then, the observation model of the natural signal X can be rewritten as

$$Y = \Phi DW + v \tag{12}$$

Additionally, concerning the reconstruction stage of the signal X, it can be solved via Bayesian statistical learning method [31]. As shown in Eq. (13), the likelihood function of the observation vector Y with respect to the sparse weight coefficient W and noise variance σ_0^2 is

$$p\left(Y|W, \sigma_0^2\right) = \left(2\pi\sigma_0^2\right)^{-\frac{M}{2}} \exp\left\{-\frac{1}{2\sigma_0^2}\|Y - \Phi DW\|^2\right\} \tag{13}$$

$$V_8 = \begin{bmatrix} +0.4354, & +0.2857, & +0.3737, & +0.2985, & -0.1949, & +0.2106, & -0.0345, & +0.6454 \\ +0.4713, & +0.1643, & +0.0905, & +0.4926, & -0.0789, & +0.0203, & -0.0153, & -0.7022 \\ +0.0837, & -0.2260, & -0.3673, & +0.5541, & +0.5934, & -0.2579, & +0.0962, & +0.2685 \\ -0.3042, & -0.3869, & -0.2155, & +0.4597, & -0.6960, & -0.0189, & -0.0942, & +0.0797 \\ -0.4301, & -0.2097, & +0.4432, & +0.2731, & +0.3172, & +0.6228, & +0.0107, & -0.1069 \\ -0.2585, & -0.0022, & +0.6453, & +0.1295, & +0.0114, & -0.7056, & +0.0381, & -0.0225 \\ -0.4868, & +0.8041, & +0.2408, & +0.2418, & +0.0000, & +0.0000, & +0.0000, & +0.0000 \\ +0.0000, & +0.0000, & +0.0000, & +0.0000, & -0.1358, & +0.0514, & +0.9894, & -0.0048 \end{bmatrix}.$$

Therefore, the maximum posterior estimates of W and σ_0^2 can be obtained through the linear regression with sparse constraints of W. According to the hierarchical prior model of relevance vector machine (RVM) algorithm, the hyper-parameter $\alpha = [\alpha_1, \alpha_2, ...\alpha_n]$ is introduced. And then, employing the Π-type maximum likelihood estimation algorithm, the iterative calculation algorithm of the mean value μ, the variance Q of the W posterior probability and the parameter α_0, α can be calculated by Eq. (14).

$$\begin{cases} \mu = \alpha_0 Q A^T Y \\ Q = \left(\alpha_0 A^T A + \Lambda\right)^{-1} \\ \alpha_i = \gamma_i \mu_i^{-2} = (1 - \alpha_i Q_{i,i}) \mu_i^{-2} \\ \alpha_0^{-1} = \|Y - A\mu\|_2^2 \cdot (n - Q_{i,i}\gamma_i)^{-1} \end{cases} \tag{14}$$

where $\alpha_0 = \alpha_0^{-2}, A = \Phi D, \Lambda = \mathrm{diag}(\alpha_1, \alpha_2, ..., \alpha_n), \gamma_i = 1 - \alpha_i Q_{i,i}$, $i \in \{1, 2, ..., n\}$. And $Q_{i,i}$ is the ith diagonal element in the variance matrix Q.

It can be seen from Eq. (14) that the values of μ, Q, α_0 and α are interdependent. When they are calculated iteratively until the cut-off condition is satisfied, the parameter estimation value of expectation can be obtained, where the mean value μ is the posterior estimation value of the sparse weight coefficient W.

In essence, Bayesian CS provides a posterior distribution of parameters rather than the point estimation, which can optimize the reliability of estimation adaptively. And this feature is not available in other compressive sensing models [32,33]. When it is introduced into the reconstruction process, the reconstruction performance will be stabilized. But meanwhile, the execution efficiency will decline to some extent because of the heavy computation of estimation, which can be regarded as a concession of pursuit of better stability.

2.3. Discrete V transform

Second degree V system is a new kind of complete orthogonal functions on the space $L^2[0, 1]$, which is constructed by the piecewise second-degree polynomial [34]. And the general term of this secondary system is defined as the Eq. (15). Later, Wang et al. introduced the 2D discrete V transform with orthogonality and multi-resolution characteristics based on this system [35]. The DVT can be expressed as Eq. (16).

$$V_{2,n}^{i,j}(x) = \begin{cases} \sqrt{2^{n-2}} V_{2,2}^{i}\left[2^{n-2}\left(x - \frac{j-1}{2^{n-2}}\right)\right], & x \in \left[\frac{j-1}{2^{n-2}}, \frac{j}{2^{n-2}}\right] \\ 0, & \text{otherwise} \end{cases} \tag{15}$$

where $i = 1, 2, 3$. $j = 1, 2, ..., 2^{n-2}$. $n = 3, 4, 5, ...$

$$P_n' = V_n \times P_n \times V_n^T \tag{16}$$

where P_n is a sub-image block of the natural image P with the sized of $n \times n$. V_n is the n-order transform matrix, and it can be obtained by performing unit orthogonalization on the matrix generated by taking points of the basis function $V_{2,n}^{i,j}(x)$ at equal intervals. And when $n = 8$, then

Precisely, since it has the multi-resolution features of multi-wavelet, the 2D DVT is employed to design a frequency-based embedding approach in our scheme. Moreover, compared with other embedding ones, the proposed embedding algorithm has the advantages of stronger robustness and larger embedding capacity.

3. Newly designed 2D discrete fractional-order chaotic map

In this section, a two-dimensional continuous chaotic system combined with trigonometric function is proposed and then generalized to fractional ones. Moreover, its chaotic performance is analyzed through a series of tests, including Kolmogorov entropy, approximate entropy and NIST randomness test suite.

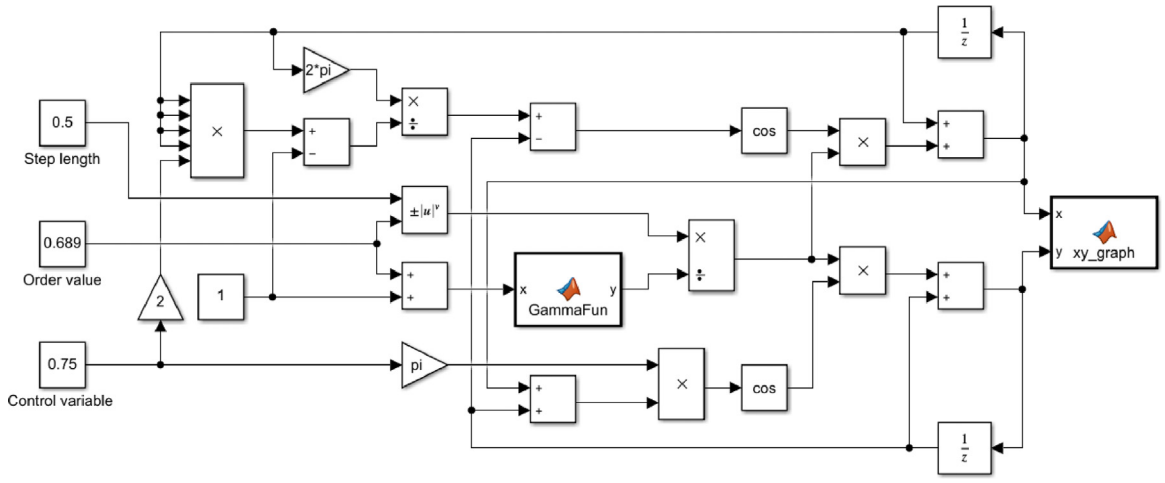

Fig. 1. Simulink model of the newly designed 2D discrete fractional-order chaotic map.

3.1. Definition of 2D-FOCM

The definition of the proposed two-dimensional chaotic system is displayed in the following equation.

$$\begin{cases} \dfrac{dx}{dt} = \cos\left(\dfrac{2\pi x}{2\mu x^4 - 1} - y\right) \\ \dfrac{dy}{dt} = \cos\left(\mu\pi\left(x + y\right)\right) \end{cases} \tag{17}$$

where μ is the control variable and x, y are the state variables of this system.

By replacing the integer derivatives of the proposed chaotic system using the fractional-order operators, Eq. (18) can be obtained, and it satisfies the Caputo fractional derivative.

$$\begin{cases} D^{\nu}x(t) = \cos\left(\dfrac{2\pi x(t)}{2\mu x(t)^4 - 1} - y(t)\right) \\ D^{\nu}y(t) = \cos\left(\mu\pi\left(x(t) + y(t)\right)\right) \end{cases} \tag{18}$$

where

$$D^{\nu}f(t) = \frac{1}{\Gamma(n-\nu)}\int_{t_0}^{t}(t-\tau)^{n-\nu-1}f^{(n)}(s)ds, \quad t > 0, \quad \nu \in (0,1)$$

Next, discretizing and differencing the Eq. (18) and the 2D discrete fractional-order chaotic map (2D-FOCM) is generated according to **Lemma 1**.

$$\begin{cases} x(n+1) = x(n) + \frac{h^{\nu}}{\Gamma(1+\nu)}\cos\left(\dfrac{2\pi x(n)}{2\mu x(n)^4 - 1} - y(n)\right) \\ y(n+1) = y(n) + \frac{h^{\nu}}{\Gamma(1+\nu)}\cos\left(\mu\pi\left(x(n+1) + y(n)\right)\right) \end{cases} \tag{19}$$

where $n \in \mathbb{N}^+$, and $h \in \mathbb{R}^+$ is the discretization step length. The Simulink model is constructed for the above-discussed discrete fractional-order system, as shown in Fig. 1, and the corresponding attractor diagram generated by this model is plotted in Fig. 2. Besides, Fig. 3 displays the chaotic sequence of proposed 2D fractional-order chaotic system. As illustrated in Figs. 2 and 3, the chaotic behavior of the newly-designed 2D-FOCM has been demonstrated.

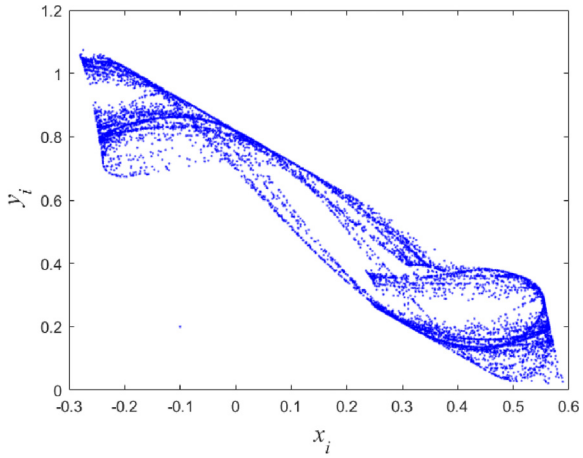

Fig. 2. Attractor diagram generated by the Simulink model.

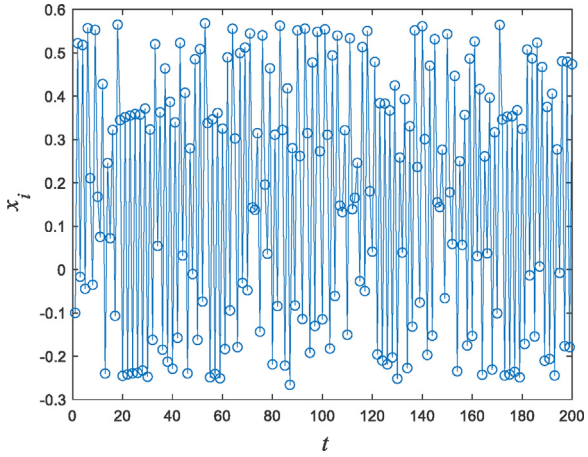

Fig. 3. Chaotic sequence of the newly designed 2D discrete fractional-order chaotic map.

3.2. Performance evaluation

3.2.1. Lyapunov exponent analysis

If the phase trajectory of nonlinear system is far from its equilibrium points, it indicates that this system is unstable. And the Lyapunov exponent (LE) is the parameter that is utilized quantificationally to describe the mutual repulsion and attraction of trajectories [36,37]. Moreover, as long as the system has a positive LE value, the chaotic motion will appear in its phase space. Conversely, when judging whether a nonlinear system is a chaotic map, just check whether its LE value is greater than 0.

In the case of $h = 0.5, \nu = 0.789, \mu = 0.75$, the Lyapunov exponential spectrum of the newly proposed 2D chaotic map solved by the LET toolbox is plotted in Fig. 4. As demonstrated in this figure,

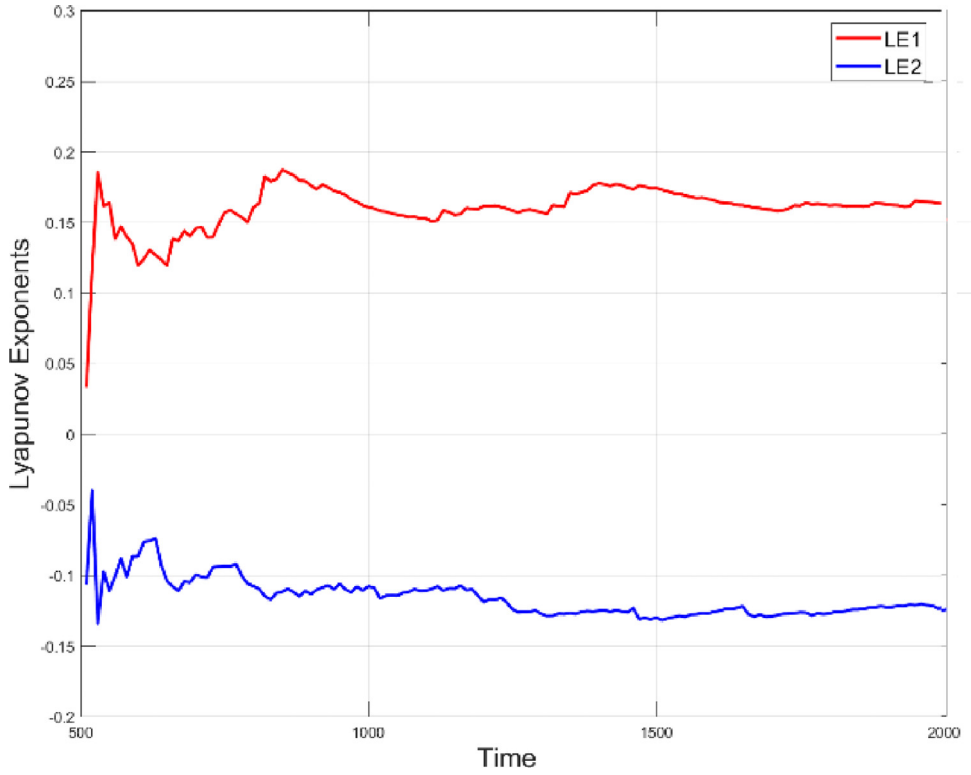

Fig. 4. Lyapunov exponent of the newly designed 2D discrete fractional-order chaotic map.

as the number of iterations increases, one of the LE values of the proposed map is always greater than 0, indicating that the discrete fractional-order nonlinear map designed in this paper does have chaotic characteristics.

3.2.2. Kolmogorov entropy analysis

The Kolmogorov entropy (KE) is a kind of entropy that evaluates the chaotic extent of a nonlinear system by testing the requested additional information to forecast future trajectories utilizing its previous states, which can be expressed by Eq. (20) [38]. If the KE value of a nonlinear system is positive, it means that there is chaotic phenomenon in this system. Moreover, the larger the KE value is, and the better its systematic complicacy is.

$$KE = -\lim_{\tau\to 0}\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n\tau}\sum_{i_1,i_2,\ldots,i_n} p(i_1,i_2,\ldots,i_n)\cdot \ln p(i_1,i_2,\ldots,i_n) \tag{20}$$

where the n and τ are respectively denoted as the embedding dimension and the time delay. Besides, $p(i_1, i_2, \ldots, i_n)$ is the joint probability. In this experiment, the G-P method recommended in Ref.[39] is utilized to calculate the value of KE. To provide an intuitional contrast, the obtained numerical results of the three testing chaotic maps with variation of their control parameters are depicted in Fig. 5. One can see form this figure that our proposed 2D-FOCM has larger LE values in the wider parameter range, compared with the remaining three chaotic maps [40–42]. It indicates that the newly designed 2D-FOCM has more sophisticated internal chaotic behavior in the two-dimensional phase plane.

3.2.3. Approximate entropy analysis

Approximate entropy (AE), reflecting the occurring likelihood of new information in a time sequence, is a measure method adopted to quantitatively assess the irregularity or complexity of time sequence [43]. Therefore, the more unpredictable time sequence corresponds to the larger the AE value. Its specific testing procedures are as follows.

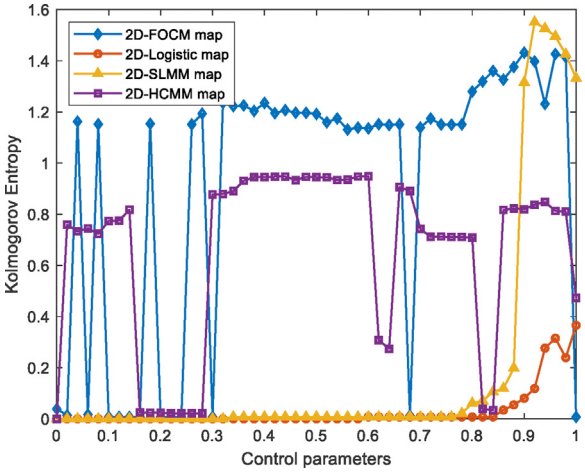

Fig. 5. The KE values of different 2D chaotic maps.

Step 1. Given a one-dimensional time sequence $\{u(i),\ i = 1, 2, \ldots, N\}$ with length of N, then this sequence is reconstructed according to Eq. (21) to generate the m-dimension vector $\{X_i,\ i = 1, 2, \ldots, N - m + 1\}$.

$$X_i = \{u(i), u(i+1), \ldots, u(i+m-1)\} \tag{21}$$

Step 2. Calculate the distance $d_m[X_i, X_j]$ between any two reconstruction vectors X_i and X_j $(j = 1, 2, \ldots, N - m + 1,\ j \neq i)$, whose mathematical definition is displayed in Eq. (22).

$$d_m\left[X_i, X_j\right] = \max_{k\in[0,m-1]} |u(i+k) - u(j+k)| \tag{22}$$

Step 3. Given a threshold r, which usually belongs to [0.2, 0.3], the number of $d_m[X_i, X_j] \leq r \cdot SD$ (SD is the standard devia-

Table 1
Test results of the sequences generated by newly designed 2D-FOCM with NIST SP800–22 suite.

Test items	P-value (x_n)	Results	*P*-value (y_n)	Results
Frequency test	0.610051	Pass	0.636927	Pass
Block Frequency test	0.780884	Pass	0.337270	Pass
Cusum-forward test	0.541582	Pass	0.513901	Pass
Cusum-reverse test	0.900263	Pass	0.584171	Pass
Runs test	0.398736	Pass	0.270025	Pass
Longest run test	0.354817	Pass	0.609395	Pass
Rank test	0.545941	Pass	0.719386	Pass
FFT test	0.508794	Pass	0.748072	Pass
Non-Overlapping template test	0.705064	Pass	0.272985	Pass
Overlapping template test	0.611951	Pass	0.317737	Pass
Universal test	0.709563	Pass	0.670276	Pass
Approximate entropy test	0.411079	Pass	0.303219	Pass
Random-excursions test ($x = -1$)	0.236432	Pass	0.851619	Pass
Random-excursions variant test ($x = 1$)	0.428361	Pass	0.688993	Pass
Serial1 test	0.375342	Pass	0.569617	Pass
Serial2 test	0.594920	Pass	0.336280	Pass
Linear complexity test	0.613804	Pass	0.400809	Pass

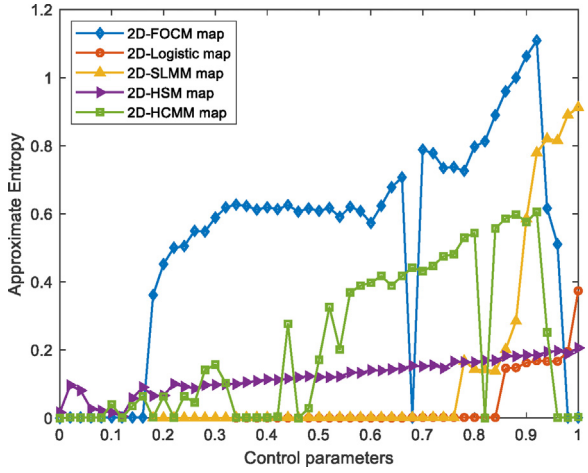

Fig. 6. The AE values of different 2D chaotic maps.

tion of the sequence u) is counted for each vector X_i, and then the ratio of it to the total number $N - m + 1$ is denoted as $C_i^{(m)}(r)$.

Step 4. Calculate the logarithmic average of $C_i^{(m)}(r)$, which is

$$\Phi^{(m)}(r) = \frac{1}{N-m+1} \sum_{i=1}^{N-m+1} \ln C_i^{(m)}(r) \tag{23}$$

Step 5. Increase the vector dimension to $m + 1$, and repeat steps (1)-(4) to obtain the $\Phi^{(m+1)}(r)$.

Step 6. Finally, for a finite time sequence u, its AE value can be determined by executing Eq. (24).

$$\mathrm{AE}(m, r, N) = \Phi^{(m+1)}(r) - \Phi^{(m)}(r) \tag{24}$$

In this experiment, the method recorded in Ref.[43] is adopted to analyze the approximate entropy of the newly-designed 2D-FOCM and other 2D chaotic maps [40–42,44]. Additionally, the comparison results of different chaotic maps are plotted in Fig. 6. It is evident that the proposed 2D discrete fractional-order chaotic map can achieve larger AEs than 2D-Logistic, SLMM, HSM and HCMM maps in most parameter settings, which sufficiently shows that the proposed 2D-FOCM map has such sophisticated chaotic properties that it is hard to be predictable. Therefore, the 2D-FOCM map is more suitable for the application in cryptographic system than those designed in Refs.[40-42,44].

3.2.4. NIST randomness test analysis

At present, most of testing methods based on statistical theory have been proposed to verify the quality of pseudo-random number sequences. In this section, the widely-used NIST SP800–22 testing suite [45] will be applied to evaluate a crucial characteristic of the proposed chaotic map, namely pseudo-randomness. It examines whether the detected time sequence generated by the chaotic map satisfies certain characteristics of the random sequence (such as periodicity, correlation, and distribution character) through probability statistics, so as to determine whether it is stochastic. Then, under the condition of that the confidence probability P_α is set to 0.01, pseudo-randomness tests are carried out on the two chaotic sequences generated by the newly designed 2D-FOCM map, and the corresponding numerical results are listed in Table 1. As can be seen from Table 1, the P-values of each test item are all greater than the confidence probability, which imply that the reliability of the chaotic sequences x_n and y_n as pseudo-random sequences is 99%. Therefore, the proposed discrete fractional-order chaotic map can simultaneously output two groups of aperiodic pseudo-random sequences.

4. 2D-FOCM-based image encryption and decryption algorithm

Conjugated the newly developed 2D-FOCM map, Bayesian compressive sensing and discrete V transform, a stable meaningful image encryption scheme is presented in this section, and its overall structure flowchart is illustrated in Fig. 7. As displayed in Fig. 7, the proposed encryption scheme consists of two stages, namely encryption and embedding. First, the key-controlled measurement matrix generated by the 2D-ICCM map [46] is utilized to compress the scrambled coefficient matrix in the wavelet packet domain, then the diffusion operation is performed to create an unrecognized image. In this stage, the volume of plain image is sufficiently abated, and the encryption process of image data is completed. Secondly, to realize the steganography of secret image, the discrete V transform-based embedding (DVT-BE) method is employed to stochastically embed the non-semantic secret image into any host image under control of the 2D-FOCM map. Additionally, in view of the linearity of CS-based compression framework, counter mode is employed to update the secret code streams in real time for withstanding the chosen-plaintext analysis attacks. And the unabridged encryption procedures are depicted detailedly as follows.

4.1. Encryption process

To make more universality, it is assumed that the resolution of the plain image $P1$ and the host image $H1$ are both denoted as $N \times$

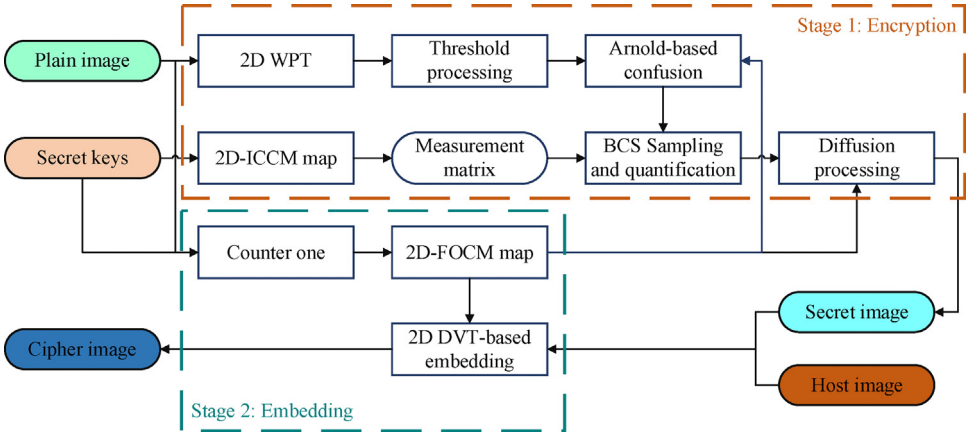

Fig. 7. The structure of encryption scheme.

N. Meanwhile, the preset compression rate is set to C_R. Moreover, it is worth mentioning that the resolution of the $H1$ is not restricted to $N \times N$. Any natural image with a resolution greater than $N \times N$ can be chosen as the host image.

4.1.1. Generating the secret code streams by counter mode

It is pointed out in the Ref.[47] that the encryption scheme can effectively withstand the chosen-plaintext attacks by working in one-time-sampling mode (OTSM). In other words, the secret keys adopted in each encryption process is never used. Thus, in our scheme, the counter mode is employed to update the secret code streams of each encryption stage to achieve the effect "One cipher image corresponds to one key". And its mathematical definition is

$$Ctr_{i+1} = Ctr_i + 1 \bmod 10^{\lambda}, \ \ i = 1, 2, 3, ..., N, \ \ l \cdot N < 10^{\lambda} \tag{25}$$

where the symbols λ and l respectively represent the security parameter and the number of images to be encrypted.

Step 1. All pixel values in the plain image $P1$ are summed and its average value is given as

$$ir = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} P1(i, j) \tag{26}$$

Step 2. Set the values of initial parameters to (x_0, y_0), $Ctr_0^{(1)}$, $Ctr_0^{(2)}$ and λ, and then referring to Eq. (27), the updated key vectors SX and SY is obtained. Note that the SX_i and SY_i are separately utilized to encrypt the ith plain image.

$$\begin{cases} SX_i = Ctr_i^{(1)} \times 10^{-4} + ir \times 10^{-3} + x_0 \bmod 1 \\ SY_i = Ctr_i^{(2)} \times 10^{-4} + ir \times 10^{-3} + y_0 \bmod 1 \end{cases} \tag{27}$$

Step 3. Under the condition that the initial states are set to SX_i and SY_i, the 2D-FOCM map is iterated $(N_0 + N^2)$ times to acquire two chaotic sequences $X = \{x_1, x_2, ..., x_{N_0+N^2}\}$ and $Y = \{y_1, y_2, ..., y_{N_0+N^2}\}$.

Step 4. By virtue of Eq. (28), three secret code streams $\{S_1, S_2, S_3\}$ are generated by operating these two chaotic sequences X and Y.

$$\begin{cases} S_1 = \mathrm{sort}\left(X_{N_0+1}^{N_0+N^2}, \text{'ascend'}\right) \\ S_2 = \left\lfloor Y_{N_0+1}^{N_0+N^2} \times 10^{10} \right\rfloor + m_0 \bmod 256 \\ S_3 = ir - X_{N_0+1}^{N_0+\lfloor C_R \cdot N \rfloor \cdot N} - Y_{N_0+1}^{N_0+\lfloor C_R \cdot N \rfloor \cdot N} \bmod 1 \end{cases} \tag{28}$$

where the symbol $\lfloor \cdot \rfloor$ represents the round-off operation approaching zero.

4.1.2. Encrypting the plain image based on BCS model and Arnold confusion

Generally speaking, there may be high correlation and data redundancy between adjacent pairs of pixels in natural images. As far as an effective image encryption scheme is concerned, it should decorrelate these high correlations and degrade redundancy to improve information transmission efficiency. Therefore, Bayesian compressive sensing controlled by the 2D-ICCM map is adopted to compress and initially encrypt the wavelet packet coefficients of plain image $P1$. Furthermore, the compressed image is encrypted again by the modulus diffusion operation to eliminate its unique statistical characteristics. Most noteworthy is that the diffusion process refers to modifying pixel values in a particular way to achieve the avalanche effect. The detailed steps are as follows.

Step 1. Compared with other sparse representation transforms, such as DCT, DWT, SWT and so on, wavelet packet transform can achieve better sparsification performance. Therefore, using DB wavelet as the base wavelet, multi-layer 2D WPT is carried out on the plain image to acquire the coefficient matrix $P2 \in \mathbb{R}^{N \times N}$.

Step 2. Before the Arnold-based confusion, the coefficient matrix $P2$ is thresholded to further enhance its sparsity. Then scrambling it according to the secret code stream S_1. The Arnold scrambling process can be expressed as

$$\begin{pmatrix} i_{n+1} \\ j_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & S_1^n \\ S_1^{N+n} & S_1^n \times S_1^{N+n} + 1 \end{pmatrix} \times \begin{pmatrix} i_n \\ j_n \end{pmatrix} \bmod \begin{pmatrix} N \\ N \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{29}$$

where the coordinates (i_n, j_n) and (i_{n+1}, j_{n+1}) respectively indicate the position before and after the confusion. Besides, the purpose of this step is to initially encrypt the coefficient matrix $P2$ on the one hand, and to relax the limited isometric constraint of measurement matrix on the other. Moreover, the coefficient matrix after scrambling is named $P3$.

Step 3. According to secret keys u_0, v_0 and sampling distance d, the ICCM map is iterated $(N_0 + (d+1) \cdot \lfloor C_R \cdot N \rfloor \cdot N)$ times to obtain two chaotic sequences $U = \{u_1, ..., u_{N_0+(d+1)\cdot\lfloor C_R \cdot N \rfloor \cdot N}\}$ and $V = \{v_1, ..., v_{N_0+(d+1)\cdot\lfloor C_R \cdot N \rfloor \cdot N}\}$. Then, a new pseudo-random sequence P_{uv} is generated by operating the chaotic sequences U and V, referring to Eq. (30).

$$P_{uv} = 1 - U(N_0 + 100 : d : \mathrm{end}) - V(N_0 + 100 : d : \mathrm{end}) \tag{30}$$

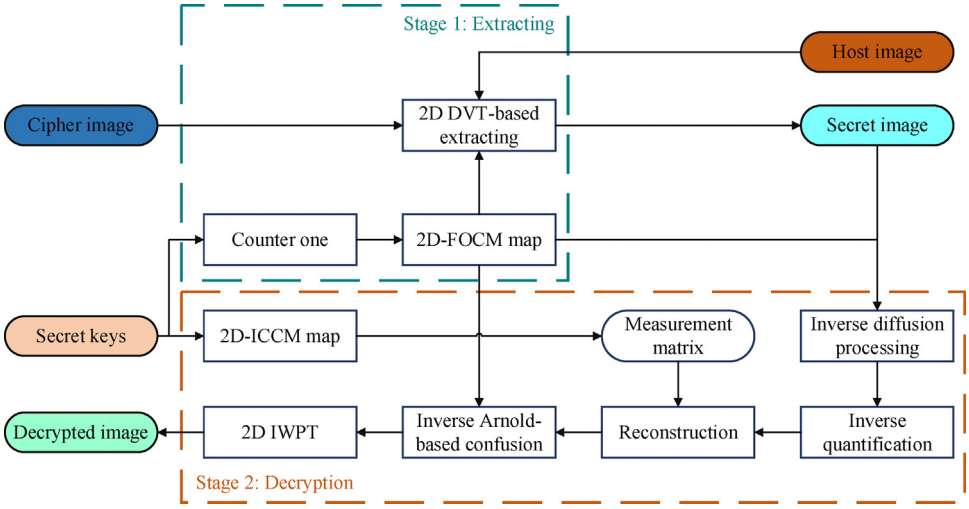

Fig. 8. The structure of decryption scheme.

Step 4. The key-controlled measurement matrix Φ is constructed according to the following equation.

$$\Phi = \sqrt{\frac{2}{\lfloor C_R N \rfloor}} \begin{bmatrix} P_{uv}(1) & P_{uv}(\lfloor C_R \cdot N \rfloor + 1) & \cdots & P_{uv}(\lfloor C_R \cdot N \rfloor \cdot (N-1) + 1) \\ P_{uv}(2) & P_{uv}(\lfloor C_R \cdot N \rfloor + 2) & \cdots & P_{uv}(\lfloor C_R \cdot N \rfloor \cdot (N-1) + 2) \\ \vdots & \vdots & \vdots & \vdots \\ P_{uv}(\lfloor C_R \cdot N \rfloor) & P_{uv}(2\lfloor C_R \cdot N \rfloor) & \cdots & P_{uv}(\lfloor C_R \cdot N \rfloor \cdot N) \end{bmatrix} \tag{31}$$

Step 5. The coefficient matrix $P3$ obtained after Arnold-based confusion is measured in parallel by use of Φ, and its corresponding mathematical equation is as follows.

$$P4 = \Phi \times P3 \tag{32}$$

Step 6. The real measurement value matrix $P4$ is linearly quantized to among 0 and 255 through the following equation, thereby acquiring the compressed image $P5$.

$$P5 = \left\lfloor \frac{255 \times (P4 - \min(P4))}{\max(P4) - \min(P4)} \right\rfloor \tag{33}$$

Step 7. Finally, the modulus operation is developed to eliminate the statistical properties of the compressed image $P5$. This step can be described by Eq. (34).

$$P6(i) = P5(i) + S_2(i) + m_1 \bmod 256 \tag{34}$$

4.1.3. Embedding the secret image into the host image

Most of the existing image encryption schemes only protect the information of image data, but neglect to encrypt the appearance of secret image, And the commonality of this kind of encryption scheme is that the generated secret image is noise-like, also has low correlation and flat histogram. When it is transmitted in the public channel or preserved in the non-secret storage media, there are certain security loopholes. Thus, in this section, a discrete V transform-based embedding method is developed to eliminate the appearance characteristics of secret image. Its specific operations are described as follows.

Step 1. The secret code stream S_3 is sorted in ascending order to generate the index sequence Ts, which is used to control the subsequent embedding operation.

Step 2. Divide the host image $H1 \in \mathbb{N}^{N \times N}$ into several non-overlapping image sub-blocks $H_2^i (i = 1, 2, ..., \lfloor N^2/n^2 \rfloor)$ with size of $n \times n$, and perform 2D DVT on each sub-blocks, as shown in Eq. (35).

$$H_3^i = V_n \times H_2^i \times V_n^{\mathrm{T}} \tag{35}$$

Step 3. Next, referring to Eq. (36), the secret image $P6$ is randomly embedded in the coefficient matrix of the host image $H1$ in transform domain. It is worth noting that multiplying the gain factor $\alpha \in \{\mathbb{R} | [0, 1]\}$ in front of the H_3^i is to prevent data overflow or underflow of steganographic image after the confidential information is embedded.

$$\begin{aligned} &H_4^i\left(\frac{1}{2}n + 1 : end,\ \frac{1}{2}n + 1 : \mathrm{end}\right) \\ &= \alpha \cdot \mathrm{H}_3^i\left(\frac{1}{2}n + 1 : \mathrm{end},\ \frac{1}{2}n + 1 : \mathrm{end}\right) \\ &\quad + (1 - \alpha) \cdot P6(Ts(j)) \end{aligned} \tag{36}$$

where $j = 1, 2, 3, ..., \lfloor C_R \cdot N \rfloor \cdot N$.

Step 4. The inverse DVT transform is performed on the sub-matrix block H_4^i carrying the secret image, which can be expressed by Eq. (37). Eventually, the cipher image $C1 \in \mathbb{N}^{N \times N}$ can be acquired by splicing each of the transformed sub-blocks H_5^i.

$$H_5^i = \mathrm{round}\left(V_n^{\mathrm{T}} \times H_4^i \times V_n\right) \tag{37}$$

where the symbol round$(\cdot)$ denotes the rounding operation.

4.2. Decryption process

The whole structure flowchart of corresponding decryption scheme is displayed in Fig. 8. It is made up of the inverse operations of encryption process. Additionally, the prerequisite of precisely recovering the plain image from the $C1$ is that the secret keys are successfully transmitted to the decrypting end through a secure channel or by means of public key encryption. Meanwhile, it can be seen from Fig. 8 that the host image is indispensable in the extraction stage. Therefore, we recommend that the host image is selected randomly from the database which is established by sender and receiver. Next, the entire decryption procedures are depicted detailedly below.

Step 1. First of all, the decrypter updates the received secret keys through the counter, and then utilizes the updated keys to control the 2D-FOCM and 2D-ICCM map for generating three secret code streams $\{S_1, S_2, S_3\}$ and the key-controlled measurement matrix Φ.

Step 2. Relying on the index sequence Ts, the secret image $P6$ is extracted from the sub-coefficient matrix block obtained by performing discrete V transform on H_5^i.

Step 3. Then, the secret image $P6$ is processed by the chaotic map-controlled inverse modulus operation for obtaining the compressed image $P5$, which can be depicted by Eq. (38).

$$P5(i) = 512 + P6(i) - S_2(i) - m_1 \bmod 256 \tag{38}$$

Step 4. Before adopting the fast RVM reconstruction algorithm to restore the wavelet packet coefficient matrix $P3$ from the compressed image $P5$ with high probability, the inverse quantization operation is first performed on it, which is defined as Eq. (39).

$$P4 = P5 \times \frac{\max(P4) - \min(P4)}{255} + \min(P4) \tag{39}$$

Step 5. Finally, the plain image $P1$ is reconstructed by manipulating the inverse wavelet packet transform (IWPT) on the coefficient matrix $P3$.

5. Simulation results

Matlab 2020b installed on the laptop with 1.8 GHz i7–8550 U CPU and 16 G RAM is employed in this section to evaluate the encryption-decryption effects of our presented scheme, and then analyze the influence of some important parameters on simulation results. In the experiments, the 512×512 sized images "Lena", "Brain", "Woman", "Peppers", "Barbara" and the 512×512 sized images "Baboon", "Goldhill", "Boat", "Sailboat", "Bridge" are stochastically selected as the plain images and the host images. Besides, the secret keys and some requisite parameters are set as follows: $[x_0, y_0] = [-0.1, 0.2], [u_0, v_0] = [0.678, 0.496], Ctr_0^{(1)} = 1126, Ctr_0^{(2)} = 236, \lambda = 3, h = 0.5, v = 0.689, \mu = 0.75, \theta = 4, Ts = 35, \alpha = 0.82, d = 25, m_0 = 178$ and $m_1 = 62$. Meanwhile, to avert the adverse effects caused by the transient effect of chaotic maps, the value of N_0 is taken as 500.

In this paper, the mean structure similarity (MSSIM) and peak signal-to-noise ratio (PSNR) [48] are employed to qualitatively assess the performance of our schemes. The mathematical definition of MSSIM is described as

$$\begin{aligned} MSSIM = \frac{1}{L} \times \sum_{i=1}^{L} & \frac{2\mu_1^i \mu_2^i + (0.01 \times 255)^2}{\left(\mu_1^i\right)^2 + \left(\mu_2^i\right)^2 + (0.01 \times 255)^2} \\ & \times \frac{2\sigma_1^i \sigma_2^i + (0.03 \times 255)^2}{\left(\sigma_1^i\right)^2 + \left(\sigma_2^i\right)^2 + (0.03 \times 255)^2} \\ & \times \frac{2\sigma_{12}^i + (0.03 \times 255)^2}{2 \times \sigma_1^i \times \sigma_2^i} \end{aligned} \tag{40}$$

where L is the total number of non-overlapping sub-blocks extracted from the image. μ_1^i and σ_1^i severally represent the mean value and variance of the ith sub-image block. Furthermore, σ_{12}^i signifies the covariance between the two sub-image blocks. As the equation shows, larger its value indicates higher the similarity between the two images.

5.1. Encryption and decryption results

The simulation results and its corresponding numerical results of our scheme are illustrated in Fig. 9 and Table 2. Look-ing from the vision perspective, it can be clearly seen that the compressed secret image with flat histogram is noise-like, and any texture information of plain image cannot be identified from it, thereby the data of the image is protected. By embedding the noise-like secret image into any visually secure host image, the generated cipher images, plotted in Fig. 9.(f1)–(f6), are visually secure. Moreover, they are highly similar to their respective host images, and the differences between them are hardly distinguished by the naked eyes. In other respects, the visual quality of the decrypted image is not significantly degraded compared to its corresponding plain image.

Table 2
PSNR and MSSIM values of simulation results.

Plain image	Host image	$PSNR_{dec}$ (dB)	$PSNR_{cip}$ (dB)	$MSSIM_{cip}$
Lena	Baboon	31.6345	32.0209	0.9337
Brain	Goldhill	36.5580	32.1895	0.8862
Woman	Boat	32.5970	32.0510	0.8847
Peppers	Sailboat	31.9318	32.1190	0.8794
Barbara	Bridge	30.3427	32.1167	0.9447
Average		**32.6128**	**32.0994**	**0.9057**

In Table 2, the symbol $PSNR_{dec}$ denotes the PSNR value between plain image and decrypted image. The symbols $PSNR_{cip}$ and $MSSIM_{cip}$ respectively denote the PSNR and MSSIM between host image and cipher image. Numerically, the average value of $PSNR_{cip}$ is greater than 32 dB and the average value of $MSSIM_{cip}$ approaches to 1. It indicates that the cipher images are basically identical with their host images in appearance. Additionally, the average value of PSNR between plain image and decrypted image is also larger than 32 dB. In short, our proposed encryption-decryption scheme has good imperceptibility as well as satisfactory reconstruction quality.

5.2. Effect of the gain factor α on simulation results

To successfully hidden the non-semantic secret image into any non-secret-involved host image, the fusion function displayed in Eq. (36) is developed. As this equation shows, the gain factor α is adopted to prevent data overflow or underflow on the one hand, and is also utilized to control the embedding ratio on the other hand. Next, the images and the secret keys illustrated in the Section 5 are employed to conduct experiments for analyzing the effect of the α on the encryption and decryption results, which is plotted in Fig. 10. Among it, the orange and purple curves represent the relationship of the PSNR between host image and encrypted image with the gain factor. Additionally, the blue and yellow curves represent the relationship of the $PSNR_{dec}$ with the gain factor. As can be seen from Fig. 10, a larger gain factor α means the better imperceptibility of cipher image, as well as the lower decryption quality. Therefore, as for most plain images, we recommend that the value of α should be between 0.8 and 0.85 to acquire a balanced encryption/decryption effect.

5.3. Effect of the measurement matrix on simulation results

How to construct a key-controlled measurement matrix that satisfies the restricted isometric property (RIP) [49] is one of the core issues of the compressive sensing theory, which will directly affect the compression performance of the proposed encryption scheme. In our scheme, the measurement matrix Φ is designed by the two-dimensional ICCM map. Therefore, the effect of the system control parameter θ on the compression performance is analyzed. In the experiment, the selected images and the secret key settings are the same as those described in Section 5. Then, the numerical results are plotted in Fig. 11. Clearly, it can be seen from this figure that as the control parameter θ varies, the value of $PSNR_{dec}$ also fluctuates, and the maximum fluctuation does not exceed 1.5 dB.

Fig. 9. Simulation results of the proposed visually meaningful encryption scheme. (a1)–(a6) are the plain images, (b1–(b6) are the host images, (c1)–(c6) are the secret images manufactured by our scheme, (d1)–(d6) are the histograms of corresponding secret images, (e1)–(e6) are the decrypted images and (f1)–(f6) are the generated visually secure cipher images.

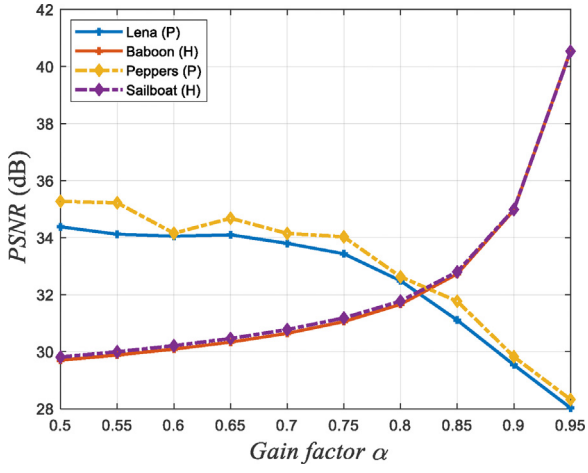

Fig. 10. PSNR vs gain factor α with different images.

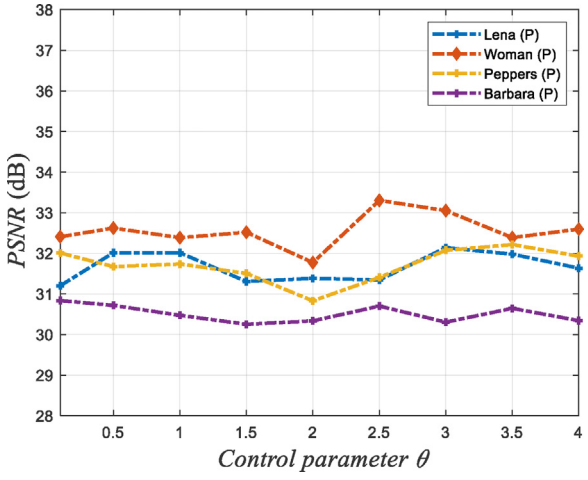

Fig. 11. PSNR vs control parameter θ with different images.

Since different plain images are of different texture features, the effect of the θ on the compression performance of various images is not identical. Furthermore, it is worth mentioning that different initial states of this chaotic map will also lead to changes in the performance of measurement matrix, but its effect on the compression performance of our encryption scheme is minimal.

5.4. Effect of compression method on simulation results

At present, existing image encryption schemes based on parallel CS or block CS usually perform further sparse processing by setting a fixed global threshold value *Ts* after frequency-domain transform [50]. However, since different natural images have different

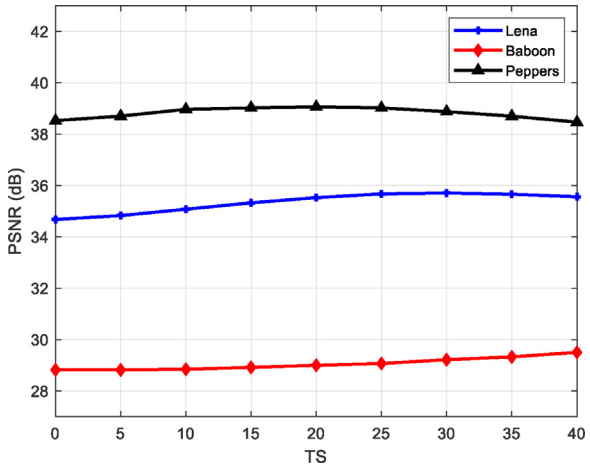

Fig. 12. PSNR vs threshold value *Ts* with different images.

Table 3
The PSNR and MSSIM values for different host images.

Plain image	Host image	$PSNR_{dec}$ (dB)	$PSNR_{cip}$(dB)	$MSSIM_{cip}$
Lena	Baboon	31.6345	32.0209	0.9337
	Goldhill	31.8195	32.1950	0.8853
	Sailboat	32.4283	32.0986	0.8794
Woman	Baboon	33.6600	32.0449	0.9344
	Goldhill	32.4650	32.2097	0.8847
	Sailboat	32.5023	32.1322	0.8788
Peppers	Baboon	32.6960	32.0280	0.9340
	Goldhill	32.2555	32.1950	0.8857
	Sailboat	31.9318	32.1190	0.8794

texture characteristics, this approach may cause the scheme performance to be unstable in terms of compressibility. To solve this issue, this paper adopts Bayesian CS to execute data dimensionality reduction. its core idea is to first assume the prior distribution for all parameters to be solved, and while the posterior information corrects the prior information, the optimal reconstruction signal is obtained by adjusting the reconstruction model in real time through the confidence coefficient of acquired parameters. In this experiment, the embedding stage is removed first, and then the plain images (Lena, Baboon, and Peppers) are encrypted separately under condition of different threshold values. The obtained experimental result is plotted in Fig. 12 below. It is obvious from the figure that with increase of the threshold value *Ts*, the visual quality of the different decrypted images fluctuate about 1 dB, which is more flat than those in Ref. [18] (about 1.5 dB), Ref. [51] (about 2 dB) and Ref. [52] (about 3 dB).

5.5. Effect of different carrier images on simulation results

In the last subsection, we will choose different host images to analyze their effect on the simulation results. The corresponding experimental data obtained are listed in Table 3. The images and secret keys used are set as what described in Section 5. As is shown in this table, encrypting different plain images and respectively embedding them into different host images has almost no effect on the imperceptibility of its secret image. But it has a certain degree of effect on visual quality of our scheme, and the maximum fluctuation is about 1 dB. Additionally, the inconsistency of reconstruction quality obtained by embedding the same secret information into different non-secret host images is caused by the irreversibility of embedding approach. Finally, it is suggested to adopt the image with rich texture information as the host image, which is conducive to enhance the imperceptibility and compression performance of scheme and avoid detection by steganography analyzer.

6. Performance analysis

In this section, the security, compressibility, robustness, and operating efficiency of proposed scheme are discussed and compared with existing state-of-the-art related encryption schemes [17,18,46,51,52] under the condition of the same dataset. The images, secret keys and parameters utilized in the experiences are set as what described in Section 5. Additionally, the most data of the comparison schemes come from the records listed in the corresponding source articles.

6.1. Security analysis

6.1.1. Key space analysis

As discussed in Ref.[53], the volume of key space of an effective image encryption scheme should be greater than 2^{100} to withstand various exhaustive attacks. In our scheme, the secret keys are mainly utilized to control the counter to update the initial states of the 2D-FOCM map and to iterate the 2D-ICCM map to generate the key-controlled measurement matrix. Assuming that the calculation accuracy in this experimental environment is 10^{-14}, the key space of our proposed scheme is greater than 2^{465}. Besides, if other parameters, such as d, m_0, m_1 and so on, are regarded as the secret keys, the total key space becomes even larger. The comparison results with other encryption schemes in terms of key space are listed in Table 4. As is shown in this table, the encryption scheme we designed has better ability to withstand the brute force attacks than those introduced in Refs.[17,18,51-53].

6.1.2. Key sensitivity analysis

As far as a sufficiently secure image encryption scheme is concerned, it should be extremely sensitive to the secret key. Namely, when the decryption key changes slightly, there is a huge visual difference among the obtained decrypted images and its respective plain image, and any texture information of the plain image is unable to acquire from it [54]. In our scheme, it relies on the sensitivity of chaotic map to the initial states to make the designed encryption scheme extremely sensitive to the secret keys. Next, the key sensitivity of the proposed decryption scheme is quantitatively evaluated by the number of pixel change rate (NPCR) [55] that is defined in the Eq. (41), and the MSSIM. Herein, images “Lena” and “Baboon” are adopted as the plain image and the host image, and the encryption keys are set as what recorded in Section 5. Then five sets of wrong secret keys which are generated by respectively adding 10^{-14} to one of the correct keys x_0, y_0, u_0, v_0, θ and keeping the rest of the keys unchanged are utilized to decrypt the cipher image.

$$NPCR = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left|\mathrm{Sign}\left(I_1^{i,j} - I_2^{i,j}\right)\right| \times 100\% \tag{41}$$

Table 4
Comparison with other schemes in terms of key space.

Schemes	Proposed	Ref. [17].	Ref. [18].	Ref. [51].	Ref. [52].	Ref. [53]
Key space	$> 2^{465}$	2^{186}	2^{249}	2.56×2^{195}	$37^2 \times 2^{296}$	2^{188}

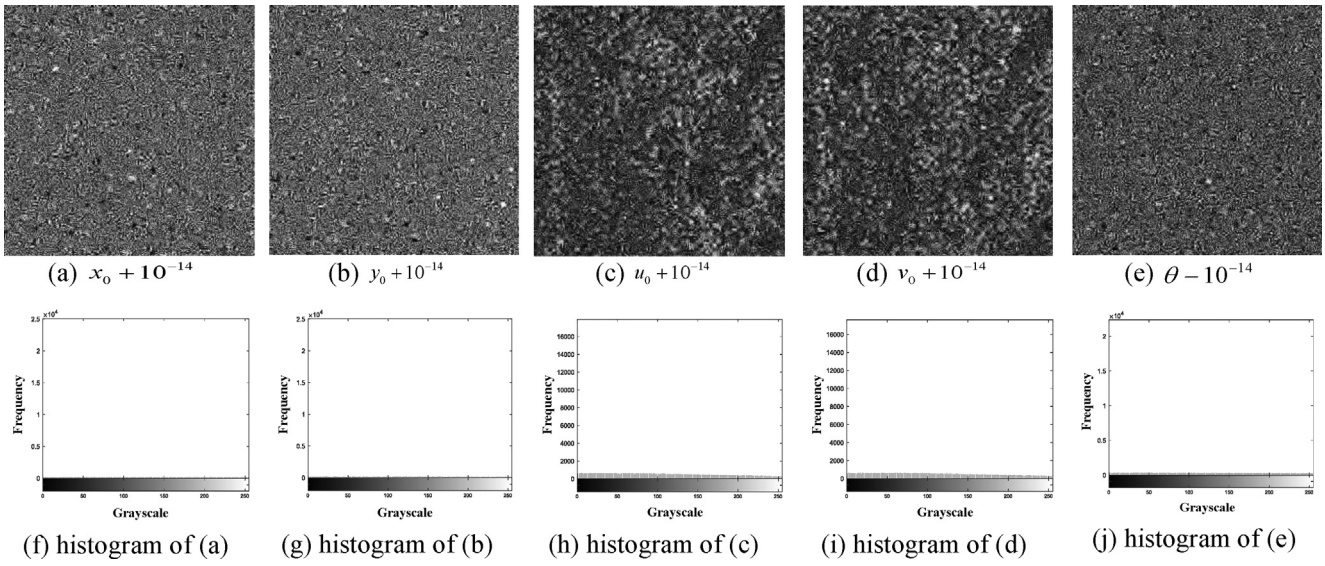

Fig. 13. Decryption results with wrong keys in key sensitivity analysis.

Table 5
The NPCR and the MSSIM between the decrypted image with wrong keys and plain image.

Decrypted image	Decryption key	$NPCR_{dec}$	$MSSIM_{dec}$
Fig. 12.a	$x_0 + 10^{-14}$	100%	0.0148
Fig. 12.b	$y_0 + 10^{-14}$	100%	0.0140
Fig. 12.c	$u_0 + 10^{-14}$	100%	0.0405
Fig. 12.d	$v_0 + 10^{-14}$	100%	0.0455
Fig. 12.e	$\theta - 10^{-14}$	100%	0.0188

Table 6
Experimental results of information entropy analysis.

Image	Information entropies	
	Plain image	Intermediate secret image
Lena	7.4464	7.9973
Brain	4.6652	7.9974
Woman	7.2695	7.9971
Peppers	7.5715	7.9973
Barbara	7.5252	7.9968
Average	**6.89556**	**7.99718**

The experimental results are displayed in Fig. 13 and Table 5. As can be seen from the results, the values of $NPCR_{dec}$ is 100% and the values of $MSSIM_{dec}$ is close to 0, any subtle change in the secret keys will cause a decrypted image that is irrelevant to the plain image. Moreover, it does not reveal the statistics information and texture information of plain image. In summary, our scheme is extremely sensitive to the secret keys in decryption process.

6.1.3. Information entropy analysis

Information entropy (IE) is commonly employed to quantitatively measure the randomness of a certain information source, and it is mathematically defined as

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \cdot \log\left(p(m_i)^{-1}\right) \tag{42}$$

where $p(m_i)$ denotes the probability of gray level m_i. Moreover, in this experiment, the variate n is equal to 256 and the ideal IE value is 8. Under the conditions that the embedding stage is remove and the compression rate is set to 0.25, the values of information entropy in five plain images are calculated and then listed in Table 6. It can be seen from the numerical results that the IE values of secret images are all greater than 7.99, indicating that the intermediate secret images generated by the proposed encryption scheme have good randomness.

6.1.4. Correlation coefficient analysis

The correlation coefficient (CC) reflects the degree of correlation between neighboring pixels in an image [56], and its mathematical definition is shown in the following Eq. (43). For a natural image, the value of its correlation coefficient often approaches 1, but this strong correlation can be destroyed by an effective image cryptosystem. Next, to assess the CCs of different images, 5000 pairs of pixels are selected for experimentations.

$$CC_{\mathbf{XY}} = \frac{E(X - E(X)) \cdot E(Y - E(Y))}{\sqrt{D(X)} \cdot \sqrt{D(Y)}} \tag{43}$$

where X and Y are the selected pixel vector with length of N, as well as $E(X) = \sum_{i=1}^{N} X_i/N$, $D(X) = \sum_{i=1}^{N} (X_i - E(x))^2/N$. The CCs diagrams and corresponding numerical results are respectively provided in Fig. 14 and Table 7. It can be seen from the experimental results that (1) The neighboring pixels in the plain image are roughly positively correlated, and its CC value is close to 1, indicating that it has a strong correlation. (2) The strong correlation in the plain image is effectively broken by our encryption scheme, resulting in a secret image whose CC value is approximately 0. (3) The secret image is embedded into the publicly available host image through DVT-BE method to realize the visual encryption of image appearance. This process is less destructive to the texture features of the host image, so that the CC value of cipher image is similar to that of the host image.

Table 7
Correlations of two adjacent pixels for different images.

	Plain image		Secret image		Host image		Cipher image	
Horizontal	0.9859	0.9824	0.0052	−0.0086	0.7622	0.9720	0.7203	0.9477
Vertical	0.9741	0.9807	0.0112	0.0133	0.8600	0.9745	0.8022	0.9490
Diagonal	0.9618	0.9687	0.0034	0.0361	0.7353	0.9597	0.6929	0.9311

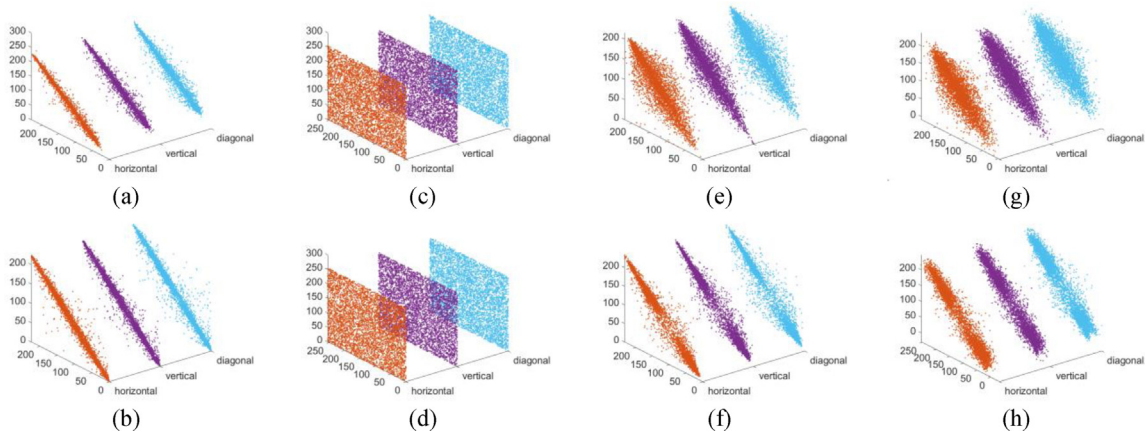

Fig. 14. Adjacent pixel pairs along the horizontal, vertical, and diagonal directions in the (a)-(b) plain images "Lena" and "Peppers", (c)-(d) respective secret images, (e)-(f) host images "Baboon" and "Sailboat", as well as (g)-(h) respective cipher image.

Table 8
Differential attack experiment results.

	Plain image	Lena	Baboon	Barbara	Boat	Peppers	Girlface
NPCR	Proposed	99.63%	99.67%	99.62%	99.64%	99.61%	99.56%
	Ref. [51].	99.56%	99.60%	99.60%	99.62%	99.59%	N/A
UACI	Proposed	33.60%	33.42%	33.57%	33 49%	33.51%	33.72%
	Ref. [51].	33.45%	33.47%	33.41%	33.45%	33.49%	N/A

6.1.5. Differential attack analysis

Differential attack refers to encrypting some artificially-constructed special plain images by encryption scheme, and then attempting to locate the connection between plain image and its cipher image by analyzing the differences between these corresponding cipher images, so as to successfully construct the plain image without using the decryption keys. In our scheme, to defend the differential attacks, the following two measures are taken. First, the embedding layer provides visual protection for the secret images, which can withstand most attacks. Then, the encryption process is relevant to the pixel value of plain image, in that the encryption keys are updated in real time through the counter mode. Next, we abolish the embedding stage and adopt the NPCR and the unified average change intensity (UACI) defined in Eq. (44) [55] to quantitatively evaluate the ability of proposed scheme in withstanding differential attacks.

$$UACI = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\frac{\left|I_1^{i,j} - I_2^{i,j}\right|}{255} \times 100\% \tag{44}$$

where I_1 and I_2 are two secret images generated by two $N \times N$ sized plain image with one bit difference. The numerical results obtained in this experiment are depicted in Table 8. It can be observed that although the difference between the two plain images is only one bit, there is a huge divergence in the generated secret images, which is larger than that of the encryption scheme introduced in Ref.[51], indicating that our encryption scheme has strong resistance capability in terms of differential attacks.

6.1.6. Visual security analysis

In the proposed scheme, in order to provide the visual protection to secret image, we embed it into a visually meaningful host image through the DVT transform-based embedding method. Therefore, the higher similarity between the generated visually secure cipher image and its original host image implies the better visual security of our scheme. In the experiments of this subsection, the values of PSNR and MSSIM among the obtained cipher images and their corresponding host images for different visually secure encryption scheme are calculated and then listed in Table 9. Obviously, it can be seen that the scheme developed in this paper can provide better visual security compared with the scheme introduced in Ref.[52]. Besides, although the mean values of MSSIM for the schemes in Refs. [46,51] are higher about 0.023 and 0.0557 than ours, their mean PSNR values are approximately less 1.4878 dB and 1.1239 dB than our scheme. Therefore, in the case of both adopting the lossy embedding approaches, the difference of encryption schemes in terms of imperceptibility is little.

6.2. Compression performance analysis

It is undeniable that the adopted Bayesian compressive sensing is a lossy image compression method, which will degrade the visual quality of reconstructed image. Therefore, in this section, we will utilize the indicator PSNR to evaluate the compression performance of the proposed scheme under the condition that the embedding stage is removed, and the corresponding numerical results are listed in Table 10. From the results, it can be seen that our encryption scheme can provide better compression performance than the other parallel or block CS-based image compression-encryption schemes developed in the Refs.[18,51,52]. Moreover, as stated in Section 5.4, the proposed scheme using the Bayesian CS is also capable of obtaining stable compression performance for plain images with different texture characteristics.

6.3. Robustness analysis

When the cipher image is transmitted over the network, it is inevitably subjected to various interferences such as data packet dropout and noise pollution, which makes it difficult to reconstruct the respective plain image. Then, this subsection evaluates the capacity of our scheme to defend against the noise attacks (NA) and the cropping attacks (CA). In the experiment, the 512×512 sized images "Girlface" and "Goldhill" are chosen stochastically as the plain image and the host image. Herein, three kinds of noise containing the salt & peppers noise (SPN), the speckle noise (SN) and the gaussian noise (GN), whose the normalized intensity are 0.0001%, 0.0003% and 0.0005% are respectively appended to ci-

Table 9
Comparison of PSNR and MSSIM values for different visually secure encryption schemes.

Plain image	Host image	$PSNR_{cip}$ (dB)				$MSSIM_{cip}$			
		Proposed	Ref. [46].	Ref. [52].	Ref. [51].	Proposed	Ref. [46].	Ref. [52].	Ref. [51]
Lena	Peppers	33.3252	31.4252	18.5136	31.7986	0.9032	0.9359	0.6726	0.9903
Airplane	Baboon	33.0562	32.5265	23.3967	32.5976	0.9586	0.9791	0.6991	0.9955
Girlface	Goldhill	33.1904	31.0570	28.2318	32.0647	0.9255	0.9496	0.7021	0.9942
Barbara	Bridge	33.1244	31.7366	25.2321	31.7397	0.9647	0.9794	0.7337	0.9946
Average		**33.1741**	**31.6863**	**23.8436**	**32.0502**	**0.9380**	**0.9610**	**0.7019**	**0.9937**

Fig. 15. Robustness test results against the noise attacks and the cropping attacks for Girlface.

Table 10
Comparison of compression performance in different image encryption schemes.

Plain image	$PSNR_{dec}$ (dB)			
	Proposed	Ref. [51].	Ref. [52].	Ref. [18].
Lena	35.7606	32.9538	31.0864	33.0984
Peppers	35.4838	33.6672	31.1202	32.6477
House	33.8724	31.9479	26.0089	32.9378
Boat	33.3123	31.7007	27.3465	32.2659
Average	**34.6073**	**32.5674**	**28.8905**	**32.7375**

pher image. Moreover, the cropping masks with the specification of 16×16, 32×32 and 48×48 are respectively placed at the center of cipher image. The simulation results are plotted in Fig. 15. The conclusion drawn from this figure is that the reconstructed plain image is visually meaningful and identifiable regardless of the intensity of noise attacks or cropping attacks on the cipher image.

Additionally, Table 11 provides the comparison results with other state-of-the-art visually meaningful image encrypt-tion schemes in terms of robustness. As can be seen from this table, (1) compared with the image encryption scheme introduced in Refs.[17,18,51], our proposed scheme has superior robustness against the GN, the SN as well as the CA. And under the same attack intensity, the fluctuation of PSNR values does not exceed 2 dB. (2) Since the embedding method and the corresponding extraction method in the Ref.[18] are completely reversible, the PSNR value of the reconstructed image is higher 5 dB than ours. In general, through simulation experiments and comparative analysis, it can be known that our proposed scheme is fully capable of withstanding certain degree of NA and CA.

6.4. Execution efficiency analysis

In the last subsection, we evaluate the time complexity and the operating efficiency of the proposed encryption scheme. In our proposed scheme, the entire encryption process is mainly composed of two stages. First, assume that the specification of plain

Table 11
Comparison of resistance capability of the noise attacks and the cropping attacks for image "Girlface".

Noise type	Attack intensity	$PSNR_{dec}$ (dB)			
		Proposed	Ref. [18].	Ref. [17].	Ref. [51]
SPN	0.0001%	28.07	33.44	33.44	31.56
	0.0003%	28.07	33.26	33.44	30.22
	0.0005%	28.07	33.02	33.44	30.02
GN	0.0001%	28.05	15.32	14.75	25.13
	0.0003%	28.00	10.19	09.35	19.41
	0.0005%	27.98	09.35	08.54	17.78
SN	0.0001%	28.07	33.44	33.44	31.56
	0.0003%	28.06	19.10	22.50	27.68
	0.0005%	28.06	15.44	17.30	24.39
CA	16×16	30.06	28.98	28.95	28.71
	32×32	28.65	24.92	24.58	27.21
	48×48	28.19	20.13	19.73	23.96

Table 12
The encryption efficiency comparison with other algorithms (Unit: s).

Item	Lena (512×512)				Lena (256×256)			
	Proposed	Ref. [18]	Ref. [17]	Ref. [51]	Proposed	Ref. [18]	Ref. [17]	Ref. [51]
Encryption	0.8125	0.9265	1.2816	0.5471	0.2026	0.1574	0.3066	0.1386
Embedding	0.0234	0.9099	0.1782	2.0184	0.0060	0.2322	0.0480	0.2596
Total	**0.8359**	**1.8364**	**1.4598**	**2.5655**	**0.2086**	**0.3896**	**0.3546**	**0.3982**

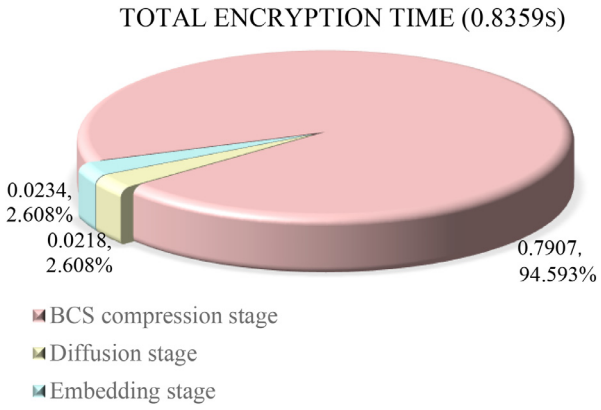

Fig. 16. Total encryption time and time consumption percentage of each part.

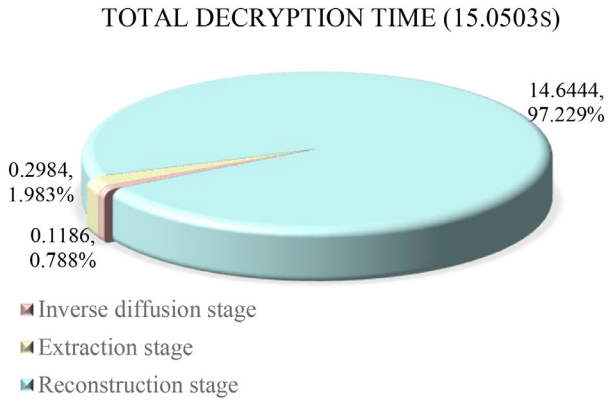

Fig. 17. Total decryption time and time consumption percentage of each part.

image and host image are both $N \times N$. Then in the first stage, it takes time complexity $\Theta(C_1 \cdot N^2)$ to create the key-controlled measurement matrix, scramble and linearly measure the coefficient matrix, as well as diffuse the compressed image. In the embedding stage, the non-semantic secret image is scrambled under control of chaotic sequence before embedding to ensure the security of its data. Moreover, the consumed time complexity of this stage is $\Theta(C_2 \cdot N^2 \cdot \log N^2)$, Among them, the sign $C_i (i = 1, 2)$ is a fixed constant. Since the $\Theta(N^2 \cdot \log N^2)$ is the largest magnitude, determining the actual execution time of algorithm, the time complexity of proposed encryption scheme is $\Theta(C_2 \cdot N^2 \cdot \log N^2)$. Additionally, it is worth mentioning that the time complexity of decryption phase largely depends on what refactoring algorithm is employed.

The gross encryption-decryption time and respective time consumption percentage of each part for plain image "Lena" are illustrated in Figs. 16 and 17. It can be seen from these two figures that in the encryption process, the BCS-based sampling occupies about 94.6% of the total operating time 0.8359 s. Furthermore, the process of decrypted image reconstructed by the fast relevance vector machine algorithm costs nearly 97.2% of the total time in decryption process. Therefore, to further enhance the operation efficiency, it is strongly recommended to divide the large-scale plain image into several sub-image blocks for encryption and decryption. Finally, Table 12 gives the comparison results of encryption efficiency in different encryption schemes. Herein, the 256×256 and 512×512 sized images "Lena" are chosen as the plain image. It can be concluded from the table that as the resolution of plain image increases, the operating time consumed also increases rapidly, but our encryption scheme all have the highest encryption efficiency compared to Refs.[17,18,51].

7. Conclusions

In this paper, by combining compressive sensing model, fractional-order chaos theory, and transform domain-based embedding technology, a stable meaningful image encryption scheme is presented. In our proposed scheme, the plaintext wavelet packet coefficients are subjected to Arnold scrambling, parallel measurement, unidirectional diffusion, and stochastic embedding to produce the final visually secure cipher image. Additionally, the ultimate goals of this work are to provide appearance protection for secret image with special visual characteristics, and to stabilize the compressibility of existing CS-based image encryption schemes under the premise of ensuring security. Eventually, security analysis

experiments indicate that the encryption scheme proposed in this paper can not only withstand chosen-plaintext attacks, but also has good decryption quality and visual security. In the future work, we will introduce the cycle generative adversarial network model (cycle GAN model) into the information security field to simultaneously encrypt and hide the digital image information.

Data availability statements

The datasets generated and analyzed during the current study are available from the corresponding author on rea-sonable request.

Declaration of Competing Interest

The authors report no conflicts of interest. The authors alone are responsible for the content and writing of this paper.

CRediT authorship contribution statement

Liya Zhu: Funding acquisition, Project administration, Supervision, Writing – review & editing. **Donghua Jiang:** Formal analysis, Methodology, Software, Writing – original draft, Writing – review & editing. **Jiangqun Ni:** Formal analysis, Resources, Writing – review & editing. **Xingyuan Wang:** Methodology, Writing – review & editing. **Xianwei Rong:** Funding acquisition, Software, Writing – review & editing. **Musheer Ahmad:** Software, Writing – review & editing. **Yingpin Chen:** Funding acquisition, Software, Writing – review & editing.

Acknowledgments

This work is supported by the National Natural Science Foundation of China [Grant No. U1736215, U1936212, 61772573], Shaanxi Province Science and Technology Program [Grant No. 2021SF-483], Natural Science Foundation of Fujian Province [Grant No. 2020J05169, 2020J01816] and Natural Science Foundation of Heilongjiang Province [Grant No. F2018022]. Last but not the least, the authors are grateful to editors and the anonymous reviewers for their valuable suggestions to improve the quality of this paper.

References

[1] Y. Zhang, P. Wang, H. Huang, Y. Zhu, D. Xiao, Y. Xiang, Privacy-assured FogCS: chaotic compressive sensing for secure industrial big image data processing in fog computing, IEEE Trans. Ind. Inf. 17 (5) (2021) 3401–3411.
[2] Y. Xian, X. Wang, L T, Double parameters fractal sorting matrix and its application in image encryption, IEEE Trans. Circuits Syst. Video Technol. (2021), doi:10.1109/TCSVT.2021.3108767.
[3] Z. Man, J. Li, X. Di, Y. Sheng, Z. Liu, Double image encryption algorithm based on neural network and chaos, Chaos Solitons Fractals 152 (2021) 111318.
[4] Y. He, Y. Zhang, X. He, X Wang, A new image encryption algorithm based on the OF-LSTMS and chaotic sequences, Sci. Rep. 11 (2021) 6398.
[5] Y. Su, X. Wang, A robust visual image encryption scheme based on controlled quantum walks, Phys. A (2021), doi:10.1016/j.physa.2021.126529.
[6] Y. Dong, X. Huang, Q. Mei, Y Gan, Self-adaptive image encryption algorithm based on quantum logistic map, Secur. Commun. Netw. 2021 (2021) 6674948.
[7] X. Wang, S Gao, A chaotic image encryption algorithm based on a counting system and the semi-tensor product, Multimed. Tools Appl. 80 (2021) 10301–10322.
[8] J. Khan, S Kayhan, Chaos and compressive sensing based novel image encryption scheme, J. Inf. Secur. Appl. 58 (2021) 102711.
[9] W. Huang, D. Jiang, Y. An, L. Liu, X. Wang, A novel double-image encryption algorithm based on Rossler hyper-chaotic system and compressive sensing, IEEE Access 9 (2021) 41704–41716.
[10] Y. Luo, J. Lin, J. Liu, D. Wei, L. Cao, R. Zhou, Y. Cao, X Ding, A robust image encryption algorithm based on Chua's circuit and compressive sensing, Signal Process. 161 (2019) 227–247.
[11] Y. Yang, J. Tian, H. Lei, Y. Zhou, W. Shi, Novel quantum image encryption using one-dimensional quantum cellular automata, Inf. Sci. (Ny) 345 (2016) 257–270.
[12] X. Xu, S Chen, A remote sensing image encryption method combining chaotic neuron and Tent map, J. Comput. (Taipei) 32 (2) (2021) 108–123.
[13] Y. Zhang, R. Zhao, X. Xiao, R. Lan, Z. Liu, X.H. Zhang, High-fidelity thumbnail-preserving encryption, IEEE Trans. Circuits Syst. Video Technol. (2021), doi:10.1109/TCSVT.2021.3070348.
[14] Y. Ding, F. Tan, Z. Qin, M. Cao, K. Choo, Z. Qin, DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption, IEEE Trans. Neural Netw. Learn. Syst. (2021), doi:10.1109/TNNLS.2021.3062754.
[15] L. Bao, Y. Zhou, Image encryption: generating visually meaningful encrypted images, Inf. Sci. (Ny) 324 (2015) 197–207.
[16] S.F. Abbasi, J. Ahmad, J.S. Khan, M.A. Khan, S.A Sheikh, Visual meaningful encryption scheme using intertwi-nning Logistic map, Adv. Intell. Syst. Comput. 857 (2018) 764–773.
[17] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy, Signal Process. 171 (2020) 107525.
[18] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, K. Nixon, An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding, Opt. Lasers Eng. 124 (2020) 105837.
[19] H. Wang, D. Xiao, M. Li, Y. Xiang, X Li, A visually secure image encryption scheme based on parallel compressive sensing, Signal Process. 155 (2019) 218–232.
[20] G. Ye, K. Jiao, X. Huang, Quantum logistic image encryption algorithm based on SHA-3 and RSA, Nonlinear Dyn. 104 (2021) 2807–2827.
[21] X.Y. Wang, S.N. Chen, Y.Q Zhang, A chaotic image encryption algorithm based on random dynamic mixing, Opt. Laser Technol. 138 (2021) 106837.
[22] R. Fay, Introducing the counter mode of operation to compressed sensing based encryption, Inf. Process. Lett. 116 (2016) 279–283.
[23] J. A.P.Artiles, D. P.B.Chaves, C Pimentel, Image encryption using block cipher and chaotic sequences, Signal Process. Image Commun. 79 (2019) 24–31.
[24] S. Rajendran, M Doraipandian, Chaotic map based random image steganography using LSB technique, Int. J. Secur. Netw. 19 (2017) 593–598.
[25] M. Hussain, A. Wahab, A. Ho, N. Javed, K. Jung, A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement, Signal Process. Image Commun. 50 (2017) 44–57.
[26] T. Wei-Liang, Y. Chia-Ming, C. Chin-Chen, Reversible data hiding based on histogram modification of pixel diff-erences, IEEE Trans. Circuits Syst. Video Technol. 19 (2009) 906–910.
[27] Q. Yang, D. Chen, T. Zhao, Y. Chen, Fractional calculus in image processing: a review, Frac. Calc. Appl. Anal. 19 (5) (2016) 1222–1249.
[28] G. Wu, D. Baleanu, S Zeng, Discrete chaos in fractional sine and standard maps, Phys. Lett. A 378 (5/6) (2014) 484–487.
[29] C. Goodrich, Existence of a positive solution to a system of discrete fractional boundary value problems, Appl. Math. Comput. 217 (9) (2011) 4740–4753.
[30] D. Donoho, Compressed sensing, IEEE Trans. Inf. Theory 52 (2006) 1289–1306.
[31] S. Ji, Y. Xue, L Carin, Bayesian compressive sensing, IEEE Trans. Signal Process. 56 (6) (2008) 2346–2356.
[32] J. Ahmad, M.A. Khan, S.O. Hwang, J.S. Khan, A compression sensing and noise–tolerant image encryption scheme based on chaotic maps and orthogonal matrices, Neural Comput. Appl. 28 (2017) 953–967.
[33] J. Ahmad, A. Tahir, J.S. Khan, A. Jameel, Q.H. Abbasi, W. Buchanan, A novel multi-chaos based compressive sensing encryption technique, in: Proceedings of the International Conference on Advances in the Emerging Computing Technologies, 2020, pp. 1–4.
[34] H. Ma, D. Qi, R. Song, T Wang, The complete orthogonal V-system and its applications, Commun. Pure Appl. Anal. 6 (3) (2007) 853–871.
[35] M. Wang, J. Zou, W Zhong, A digital watermarking method based on second degree V system, J. North China Univ. Technol. 1–5+ 3 (2006) 40.
[36] M.J. Barani, P. Ayubi, M.Y. Valandar, B.Y Irani, A new Pseudo random number generator based on generalized newton complex map with dynamic key, J. Inf. Secur. Appl. 53 (2020) 102509.
[37] B.Y. Irani, P. Ayubi, F.A. Jabalkandi, M.Y. Valandar, M.J Barani, Digital image scrambling based on a new one-dimensional coupled sine map, Nonlinear Dyn. 97 (2019) 2693–2721.
[38] Z. Hua, F. Jin, B. Xu, H. Huang, 2D Logistic-Sine-coupling map for image encryption, Signal Processing 149 (2018) 148–161.
[39] P. Grassberger, I. Procaccia, Estimation of the Kolmogorov entropy from a chaotic signal, Phys. Rev. A 28 (4) (1983) 2591.
[40] Y. Wu, J. Noonan, G. Yang, H Jin, Image encryption using the two-dimensional logistic chaotic map, J. Electron. Imaging 21 (1) (2012) 013014.
[41] Z. Hua, Y. Zhou, C. Pun, C. Chen, 2D sine logistic modulation map for image encryption, Inf. Sci. (Ny) 297 (2015) 80–94.
[42] Y. Liu, Z. Qin, X. Liao, J Wu, A chaotic image encryption scheme based on Hénon-Chebyshev modulation map and genetic operations, Int. J. Bifurc. Chaos 30 (06) (2020) 2050090.
[43] S. Pincus, Approximate entropy (ApEn) as a complexity measure, Chaos 5 (1995) 110–117.
[44] J. Wu, X. Liao, Bo. Yang, Image encryption using 2D Hénon-sine map and DNA approach, Signal Process. 153 (2018) 11–23.
[45] A. Iwasaki, Analysis of NIST SP800-22 focusing on randomness of each sequence, JSIAM Lett. 10 (2018) 1–4.
[46] D. Jiang, L. Liu, X. Wang, X Rong, Image encryption algorithm for crowd data based on a new hyperchaotic system and Bernstein polynomial, IET Image Process. 15 (14) (2021) 3698–3717.
[47] L. Zhang, K. Wong, Y. Zhang, J Zhou, Bi-level protected compressive sampling, IEEE Trans. Multi Media 18 (9) (2016) 1720–1732.
[48] M.Y. Valandar, M.J. Barani, P Ayubi, A fast color image encryption technique based on three-dimensional chaotic map, Optik (Stuttg) 193 (2019) 162921.

[49] R. Baraniuk, Compressive sensing, IEEE Signal Process. Mag. 24 (2007) 118–121.
[50] Z. Hua, K. Zhang, Y. Li, Y. Zhou, Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing, Signal Process. 183 (2021) 107998.
[51] L. Zhu, H. Song, X. Zhang, M. Yan, T. Zhang, X. Wang, J Xu, A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding, Signal Process. 175 (2020) 107629.
[52] X. Chai, Z. Gan, Y. Chen, Y Zhang, A visually secure image encryption scheme based on compressive sensing, Signal Process. 134 (2017) 35–51.
[53] M. Farah, A. Farah, T Farah, An image encryption scheme based on a new hybrid chaotic map and optimized substitution box, Nonlinear Dyn. 99 (2020) 3041–3064.
[54] F. Musanna, D. Dangwal, S Kumar, A novel chaos-based approach in conjunction with MR-SVD and pairing function for generating visually meaningful cipher images, Multimed. Tools Appl. 79 (2020) 25115–25142.
[55] A. Toktas, U Ustun, An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm, Nonlinear Dyn. 105 (2021) 1885–1909.
[56] X.H. Gao, Image encryption algorithm based on 2D hyperchaotic map, Opt. Laser Technol. 142 (2021) 107252.