IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 11, 2018, accepted November 25, 2018, date of publication November 29, 2018,
date of current version December 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2884013

A Double-Image Encryption Scheme Based on Amplitude-Phase Encoding and Discrete Complex Random Transformation

YULING LUO[1], SHUNBIN TANG[1], XINGSHENG QIN[1], LVCHEN CAO[2], FRANK JIANG[1,3,4], AND JUNXIU LIU[1], (Member, IEEE)

[1]Faculty of Electronic Engineering, Guangxi Normal University, Guilin 541004, China
[2]School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China
[3]Colleges and Universities Key Laboratory of Intelligent Integrated Automation, Guilin University of Electronic Technology, Guilin 541004, China
[4]School of Information Technology, Deakin University, Geelong, VIC 3125, Australia

Corresponding author: Junxiu Liu (j.liu@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grants 61801131, 61661008, and 61762018, in part by the Guangxi Natural Science Foundation under Grants 2017GXNSFAA198180 and 2016GXNSFCA380017, in part by the Funding of Overseas 100 Talents Program of Guangxi Higher Education under Grants F-KA16035 and F-KA16016, in part by the Doctoral Research Foundation of Guangxi Normal University under Grant 2016BQ005, in part by the Science and Technology Major Project of Guangxi under Grant AA18118004, in part by the Colleges and Universities Key Laboratory of Intelligent Integrated Automation, Guilin University of Electronic Technology, China, under Grant GXZDSY2016-03, and in part by the Research Fund of Guangxi Key Lab of Multi-Source Information Mining and Security under Grant 18-A-02-02.

ABSTRACT In this paper, a novel double image encryption scheme based on amplitude-phase encoding and discrete complex random transform (DCRT) is proposed. First, two images are merged into a plural matrix by precoding, and the synthetic signal is modulated by the phase mask which is calculated from Chen chaotic sequences generated by using the self-adapting parameter as initial values. Then, the modulated signal is encrypted by amplitude-phase encoding and the DCRT. The final cipher-text is decomposed into amplitude and phase to obtain two encrypted images. Experimental results and performance analysis show that the proposed encryption scheme can effectively resist different attacks such as the differential attack, statistical attack, and so on, and it can be used for the secure communications.

INDEX TERMS Double-image encryption, amplitude-phase encoding, DCRT, self-adapting parameter.

I. INTRODUCTION

Image data has been playing an increasingly important role in the field of information transmission and acquisition. However, it has a strong correlation between the adjacent pixels and contains a high redundancy, especially in big data era, which causes it is vulnerable to various kinds of attacks in the transmission process. Even though some traditional encryption algorithms such as data encryption standard (DES), rivest shamir adleman (RSA), have high security and mature verification, there is no consideration of the image data feature to make it be poor robustness [1]. Therefore, some new encryption theory and scheme have been successively proposed, one of which is the chaos-based cryptography because it has good characteristics of randomness, ergodicity, and sensitivity to initial conditions and is suitable for the two dimensional data processing [2]–[9].

Hence, a number of chaos-based image encryption algorithms have been proposed, for example, image encryption scheme about the chaos and DNA encoding-based [10]–[13]. and combing compressive sensing (CS) with chaotic system are developed [14], [15]. Furthermore, some new chaos-based image encryption methods combined with physical phenomenon have been designed [16], [17]. Most of these chaos-based image encryption schemes are implemented in the pixel domain which results in a limited data property. Therefore, some optical feature and optical transformation-based image encryption schemes have been further proposed to make the processing object more flexible. These algorithms can encrypt other data features of image, such as amplitude and phase [18], frequency [19], polarization state [20] and so on. Simultaneously, these encryption schemes always apply with some optical transform (e.g., fractional Fourier transform (FrRT) [21], fractional Hartley transform (HT) [22], Gyrator transform (GT) [23]) to further improve the performance of algorithm. Undeniably, most optical transform based on optical feature are linear transformation to easily make the designed encryption system weak in resisting the chosen and known plain-text attacks [24], [25].

Therefore, some novel encryption schemes which combined the optical transform with chaos [26], [27] have been presented. Specifically, in [26], the grayscale image is encrypted via combining improper HT and two random phase masks that is generated by chaotic system. Furthermore, in [27], an image encryption system utilizing the GT, chaotic phase masks, and the random shuffle about the Jigsaw transform (JT) is designed. Besides, the multiple-image encryption algorithm (MIE) [28]–[30] is the special design idea among them for the image encryption schemes except for the single-image encryption algorithms (SIE) because it can improve the encryption efficiency.

As a special case of MIE, the double-image encryption scheme has been widely concerned and applied. For example, a double-image encryption by utilizing GT and the operation of chaos-based pixel scramble is published [31]. In addition, the double-image encryption system combined logistic maps with nonlinear non-DC joint FrRT correlator is devised in [32]. Han *et al.* [33], [34] designed two chaos-based self-adaptive double colour-image encryption algorithm. Besides, the discrete fractional random transform (DFrRT) is also widely applied in the double-image encryption research [25], [35], [36]. However, the histogram of the encrypted image is not evenly distributed in [25] and [33]–[36], and the imbalances of histogram can be seen about the amplitude encrypted image and the phase encrypted image in [35] and [36], thus the capacity of resisting statistical attacks are relatively weak.

Synthesized the above discussion, a new double-image encryption scheme is proposed which is based on the amplitude-phase encoding and discrete complex random transformation (DCRT). Specifically, the chaotic sequences are firstly generated by using the self-adapting parameter to adjust the initial values of chaotic system. After that, two random phase masks are obtained by quantifying the chaotic sequences and modulated a plural signal which is generated by precoding two plain-images. Then the modulated plural signal is transformed by DCRT, and its amplitude weight and phase weight are extracted to be encoded separately. Finally, combine the new amplitude with the new phase in terms of the phase function to get the final cipher-text by modulating it with the phase mask, including the phase encrypted image and amplitude encrypted image. In summary, the contributions of this paper can be described as: (1) The self-adapting parameter that associated with the plain-image is designed, which is used in this encryption system that enhancing the ability to resist the differential attack. (2) The amplitude-phase encoding based on the chaos-based scrambling and optical amplitude-phase modulation is proposed, and it makes the structure of encryption system takes on nonlinear. (3) DCRT based on DFrRT is designed, and its order of DCRT is plural, which improves the degree of freedom of encryption and its random kernel matrix has stronger randomness than DFrRT. (4) Simulation results and performance analysis of encryption system is detailed.

The remaining chapters of this paper are organized as follows: In Section II, the fundamental knowledge is introduced, which includes the Chen chaotic system, 2D Logistic map, the self-adapting parameter and self-adapting phase masks. The proposed double-image encryption scheme and the corresponding decryption process are presented in Section III. In Section IV, the numerical simulation and performance analysis are reported. Moreover, the conclusion is provided in Section V.

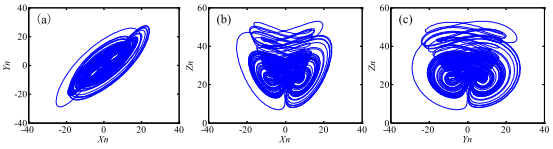

FIGURE 1. The attractors of the Chen chaotic system. (a) In x and y plane, (b) in x and z plane, (c) in y and z plane.

II. PRELIMINARIES

A. CHEN CHAOTIC SYSTEM

Chen discovered a chaotic attractor, and he finds that it's similar to the Lorenz chaotic system but the topology is not equivalent [37], [38]. The equation of Chen system is described by

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where a, b, c are the real parameters of the system, and the system is in a state of chaos when $a = 35$, $b = 3$, and $c = 28$. The phase distribution of the system is shown in Fig. 1. In this paper, the three chaotic sequences are generated through the Chen chaotic system, which are used to obtain the self-adapting phase masks and scramble the amplitude and phase.

B. 2D LOGISTIC MAP

The 2D Logistic map [35] can be described by

$$\begin{cases} x_{n+1} = \mu_1 x_n(1 - x_n) + r_1 y_n^2 \\ y_{n+1} = \mu_2 y_n(1 - y_n) + r_2(x_n^2 + x_n y_n)), \end{cases} \tag{2}$$

when $2.75 < \mu_1 < 3.4$, $2.75 < \mu_2 < 3.45$ and $0.15 < r_1 < 0.21$, $0.13 < r_2 < 0.15$, this system is in a chaotic state. In this encryption scheme, due to a small value range, r_1 is set as 0.19, and r_2 is set as 0.14, which do not act as external key. The generated two chaotic sequences x and y ($x, y \in (0, 1]$) are used to introduce the random matrix of DCRT.

C. DISCRETE COMPLEX RANDOM TRANSFORM (DCRT)

The DCRT is proposed on the basis of discrete fractional random transform (DFrRT). It can not only change the data type of the order, but also make the eigenvalue diagonal matrix be divided into two parts to enhance the randomness. The DCRT of signal $f(x)$ can be written as the format of matrix multiplication, which can be denoted by

$$R^{\alpha} f(x) = R^{\alpha} * f(x) \quad or\, f(x) R^{\alpha} = f(x) * R^{\alpha}, \tag{3}$$

where R^α is the kernel matrix of the DCRT, and α indicates a plural order ($\alpha = a' + b'i$, where $a', b' \in [-1, 1]$, $a' \neq b'$). The difference between DCRT and its inverse transform depends on the order of transformation. Here, the order of inverse transformation is $-\alpha$.

R^α can be written by

$$R^\alpha = VD^\alpha V^T, \tag{4}$$

where V is the eigenvector matrix, and $VV^T = U$, U is the unit matrix. Supposing $N \times N$ is the size of the plain-image, and if N is even number, D^α will be an eigenvalue diagonal matrix which is denoted by

$$D^\alpha = [D_1^\alpha, D_2^\alpha], \tag{5}$$

when $n = 0, 1, 3...N-1$, D_1^α can be expressed as

$$diag\{1, exp(\frac{-2\pi i(a'-b')}{T}), ..., exp(\frac{-2n\pi i(a'-b')}{T})\}, \tag{6}$$

besides, $n = 2, 4...N-2$, D_2^α can be written as

$$diag\{exp(\frac{2\pi i(b'-a')}{T}), ..., exp(\frac{n\pi i(b'-a')}{T})\}, \tag{7}$$

where $[D_1^\alpha, D_2^\alpha]$ denotes D_1^α and D_2^α are combined for a new matrix D^α, and T is the cycle of DCRT, and it's a positive number that usually be taken $T = 1$. The randomness of the transformation comes from the matrix V, which is obtained by the eigenvectors of a symmetric random matrix S, and S is constructed by a $N \times N$ random matrix E, the detailed computing process is

$$\begin{cases} E = \varepsilon * x' * y' \\ S = \dfrac{E * E^T}{2} \\ [V, d] = eig(S), \end{cases} \tag{8}$$

where ε is counted as a secret key and it satisfies the requirement of $\varepsilon \in [0, 1]$, the random sequences x', y' with size of $1 \times N^2$ can be generated by 2D Logistic map and they are reshaped into $N \times N$ matrixes, and $eig(S)$ denotes the operation of extracting eigenvalue d and eigenvector matrix V.

D. SELF-ADAPTING PARAMETER

In order to improve the ability of resisting differential attacks and strengthen the correlation with the plain-image of this encryption scheme, the self-adapting parameter is set up. The self-adapting parameter should be arranged in a certain range of data values, and the rule of self-adapting is elaborated by

$$\sigma_{adinit} = \frac{mod((sum(I_1) + sum(I_2))/2, 256)}{255}, \tag{9}$$

where I_1, I_2 are plain-images, and σ_{adinit} is used as the initial value of the Chen system and its range is from 0 to 1. It means that x_0, y_0, $z_0 = \sigma_{adinit}$. Considering that the value range of the 2D Logistic random sequences are small, hence the initial values of 2D Logistic system should satisfy

$$x_0' = a + 0.01\sigma_{adinit}, \tag{10}$$

$$y_0' = b + 0.01\sigma_{adinit}, \tag{11}$$

where a, b are constant which range from 0 to 1. Besides, the order of DCRT is indicated by

$$\alpha = means(I), \tag{12}$$

$$\beta = a' + b'i - 0.01\sigma_{adinit} + 0.01\sigma_{adinit}i, \tag{13}$$

where I is a plural synthesized signal about I_1 and I_2 with size of $N \times N$, and $means(I)$ denotes the mean values of I. Thus a slight change of plain-image can make the initial value of chaotic system, the order of DCRT and the phase masks would be different, which will result in a different encrypted image.

E. SELF-ADAPTING PHASE MASK

The $N \times N$ plain-images I_1, I_2 and the Chen chaotic system with initial values of x_0, y_0, z_0=σ_{adinit} are used to derive the phase mask.

Firstly, iterate the system in Eq. 1 for $((N \times N)/2 + 500)$ times, then discard the former 500 elements of the chaotic sequences to construct the matrixes x, y, z and quantify them by:

$$\begin{cases} h = mod(floor(x * 10^{14}), 255) + 1 \\ h_1 = mod(floor(y * 10^{14}), 255) + 1 \\ h_2 = mod(floor(z * 10^{14}), 255) + 1, \end{cases} \tag{14}$$

where h, h_1, h_2 are the quantified sequences and they are reconstructed by

$$a_1 = [h, h_1], \quad b_1 = [h_1, h_2], \quad c_1 = [h_2, h], \tag{15}$$

where $[h, h_1]$ denotes h and h_1 are combined for a $1 \times N^2$ sequence a_1.

After that, reshape I_1, I_2 into $1 \times N^2$ integer sequence I_1^*, I_2^*, and execute the XOR operation with random sequences b_1, c_1 to obtain the phase mask M_1, M_2. Firstly, the matrix I_2^* is replaced by

$$\begin{cases} I_2^*(1) = bitxor(mod(I_2^*(1) + c_1(1), 256), c_1(1)) \\ I_2^*(j+1) = bitxor(I_2^*(j), c_1(j)) \\ I_2^* = double(I_2^*/255), \end{cases} \tag{16}$$

where $bitxor(A, B)$ represents the operation of XOR between A and B, $mod(A, B)$ returns the modulus after division of A by B, and $double(A)$ returns the double-precision value for A.

Hence the mask M_1 can be obtained by

$$M_1 = exp(2\pi i * I_2^*). \tag{17}$$

Similarly, the matrix I_1^* is replaced by

$$\begin{cases} I_1^*(1) = bitxor(mod(I_1^*(1) + b_1(1), 256), b_1(1)) \\ I_1^*(j+1) = bitxor(I_1^*(j), b_1(j)) \\ I_1^* = double(I_1^*/255), \end{cases} \tag{18}$$

then the mask M_2 can also be obtained by

$$M_2 = exp(2\pi i * I_1^*). \tag{19}$$

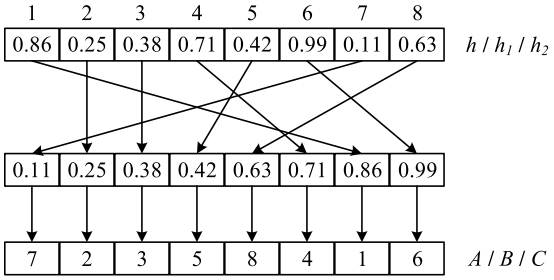

FIGURE 2. The generation process of permutation position sequence.

As shown above, the phase masks M_1 and M_2 are related with plain-image and then they are reshaped into a $N \times N$ matrix for facilitating subsequent calculations.

Besides, the permutation position sequences A, B, C can be obtained by sorting the sequence h, h_1, h_2 in ascending order and recording the corresponding index.

$$\begin{cases} h = h(1:N) \\ h_1 = h_1(1:N) \\ h_2 = h_2(1:N). \end{cases} \tag{20}$$

The detailed process for a simple example is shown in Fig. 2.

III. PROPOSED IMAGE ENCRYPTION SCHEME

A. ENCRYPTION PROCESS

The overall diagram of the proposed double images encryption scheme is shown in Fig. 3. Some images are taken as examples and the detailed procedures are described in the following steps.

- *Step 1:* The self-adapting parameter is utilized to adjust the initial value of chaotic system, and then corresponding chaotic sequences are generated, and these sequences are used to produce the phase masks M_1 and M_2 by Section II-E.
- *Step 2:* Pre-processing: Without loss of generality, the size of two plain-images is supposed to be $M \times N$ and they are denoted as I_1 and I_2. If $N \neq M$, the plain image can be reshaped to a square. For example, when $N > M$, the pixel information from the 1th to $(N-M)$th row can be copied to the rows from $(M+1)$th to Nth row of the plain image and then a square image with the size of $N \times N$ can be obtained. A similar process can be applied to the images with $N < M$.
  After the plain-images are reshaped, the pixel values of plain-image I_1, I_2 are quantified in a range of 0 to 1. Second, I_2 is encoded into phase matrix, which is multiplied by I_1 to get the synthesized signal I. The operation method is

$$I = I_1 \cdot exp(i\pi I_2), \tag{21}$$

  where "$\cdot$" denotes the element-by-element multiplication.
- *Step 3:* Use the mask M_1 to modulate the signal I and calculate the modulated signal by DCRT.

$$\begin{cases} E_0 = R^{\alpha} * (I \cdot M_1) \\ E_{01} = PT(E_0) \\ E_{02} = PR(E_0), \end{cases} \tag{22}$$

  where α stands for the order of DCRT and it is calculated by Eq. 12, $PT()$ denotes the phase-truncate, and $PR()$ denotes the phase-reserved operation, E_{01} is amplitude of E_0, and E_{02} is phase of E_0.
- *Step 4:* Utilize the phase mask M_2 to modulate E_{01} and then transform it by DCRT to get E_1.

$$\begin{cases} E_1 = (E_{01} \cdot M_2) * (R^{\beta})^T \\ E_{11} = PT(E_1) \\ E_{12} = PR(E_1), \end{cases} \tag{23}$$

  where β is the order of DCRT and it can be obtained by Eq. 13. Moreover, separate E_1 from phase E_{12} and amplitude E_{11}.
- *Step 5:* Change E_{11} and E_{12}, respectively. Firstly, E_{12} is converted into E'_{12}.

$$E'_{12} = abs(\frac{E_{12}}{\pi}), \tag{24}$$

  secondly, scramble the amplitude E_{11} and E'_{12}. The pseudo code is as follows,

Algorithm 1 Scramble E_{11} and E'_{12}

Input: $\mathbf{E_{11}}, \mathbf{E'_{12}}, \mathbf{N}$.
Output: $\mathbf{E_{11}}, \mathbf{E''_{12}}$

```
for each j ∈ [0, N − 1] do
    for each k ∈ [0, N − 1] do
        temp ← E11(A(j), B(k))
        E11(A(j), B(k)) ← E'12(B(j), C(k))
        E'12(B(j), C(k)) ← temp
    end for
end for
return E'11 ← E11, E''12 ← E'12
```

  The above pseudo code completes the numerical exchange operation of E_{11} and E'_{12}. Where A, B, C are index sequences in term of Fig 2, and the new matrix E'_{11} and E''_{12} denote E_{11} and E'_{12} after scrambling, E''_{12} is a secret key and E'_{11} is a new amplitude.
- *Step 6:* The above E_{02} and E_{12} are used, thus the secret key w is generated by

$$\begin{cases} M = \dfrac{M_1 + M_2}{2} \\ w = angle(M) + E_{02}. \end{cases} \tag{25}$$

  Set $\phi = E_{12} - w$ as a new phase, and combine the new amplitude E'_{11} to form a new synthetic signal, moreover,

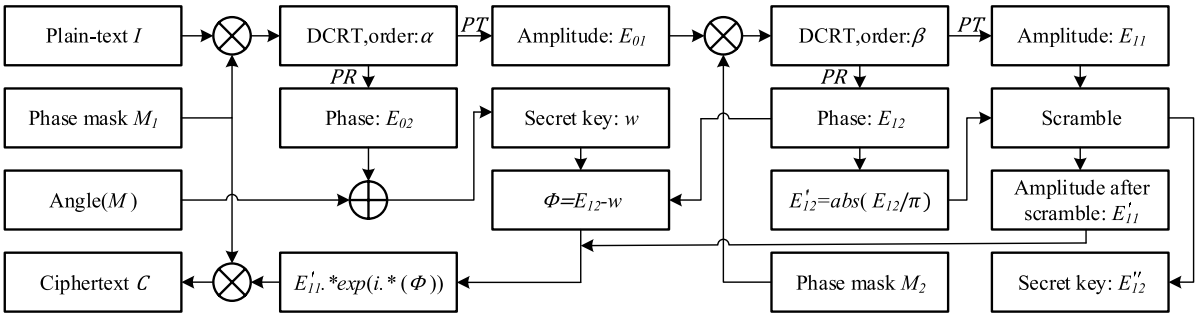

FIGURE 3. The overall diagram of this encryption scheme.

the phase mask M_1 is utilized to modulate it and obtain the final cipher-text C:

$$C = (E'_{11} \cdot exp(1i\phi)) \cdot M_1. \tag{26}$$

- *Notes:* In order to display the cipher-image conveniently, the cipher-text C is decomposed into amplitude C_1 and phase C_2:

$$\begin{cases} C_1 = abs(C) \\ C_2 = \dfrac{angle(C)}{\pi}, \end{cases} \tag{27}$$

where $C_1 \in [0, 1]$, $C_2 \in [-1, 1]$. In addition, in order to map it to the range from 0 to 255, the corresponding mapping should be taken.

$$\begin{cases} C'_1 = round(abs(C_1) * \dfrac{255}{C_{1max}}) \\ C'_2 = round((C_2 + abs(C_{2min})) \\ \qquad * \dfrac{255}{max(C_2 + abs(C_{2min}))}), \end{cases} \tag{28}$$

where $C_{1max} = max(C_1)$, $C_{2min} = min(C_2)$, $C'_1, C'_2 \in [0, 255]$. Besides, in order to enhance the safety, the secret keys w and E''_{12} are updated to get two new secret keys by

$$\begin{cases} key_1 = 0.01\sigma_{adinit} * w + angle(M) \\ key_2 = 0.01\sigma_{adinit} * (x' * E''_{12}) + angle(M), \end{cases} \tag{29}$$

the operation of restoring the key w and E''_{12} is:

$$\begin{cases} w = \dfrac{key_1 - angle(w)}{0.01\sigma_{adinit}} \\ E''_{12} = \dfrac{key_2 - angle(M)}{0.01\sigma_{adinit} * x'}. \end{cases} \tag{30}$$

B. DECRYPTION PROCESS

The key to decryption is the use of w and E''_{12}, and the schematic of the decryption process is shown in Fig 4, which is the reverse operation of encryption process. In the decryption process, the conjugation of phase masks M_1, M_2 are represented as the phase masks M_1^*, M_2^*, and the secret key w and E''_{12} are restored according to Eq. 30 firstly.

- *Step 1:* Recombine C_1 and C_2 to get the cipher-text C, then do a dot product between C and M_1^*.

$$\begin{cases} C' = C \cdot M_1^* \\ E'_{11} = PT(C') \\ \phi = PR(C'). \end{cases} \tag{31}$$

- *Step 2:* The matrix E'_{11} and ϕ are used to rebuild E_{11} and E_{12}. Firstly, scramble E'_{11} and E''_{12} to get the E_{11}, the corresponding pseudo code as follows.

Algorithm 2 Inverse scramble

Input: $\mathbf{E'_{11}}$, $\mathbf{E''_{12}}$, $\mathbf{N}$
Output: $\mathbf{E_{11}}$

```
for j ← N − 1 to 0 do
    for k ← N − 1 to 0 do
        temp ← E'11(A(j), B(k))
        E'11(A(j), B(k)) ← E''12(B(j), C(k))
        E''12(B(j), C(k)) ← temp
    end for
end for
return E11 ← E'11
```

The following pseudo code is the inverse process of the scramble in encryption scheme, and E_{11} can be obtained by it. Secondly, combine the secret key w and ϕ to reconstruct E_{12} as follows:

$$E_{12} = \phi + w. \tag{32}$$

- *Step 3:* Restore E_{01} and E_{02}: Firstly, w and M are utilized to calculated E_{02}.

$$E_{02} = w - angle(M). \tag{33}$$

Secondly, using E_{11} to dot-multiply the function that is consist of E_{12}, and transform it by the inverse DCRT.

$$\begin{cases} E'_{01} = (E_{11} \cdot exp(i * E_{12})) * (R^{-\beta})^T \\ E_{01} = E'_{01} \cdot M_2^*, \end{cases} \tag{34}$$

then it is modulated with M_2^* to get a modulated signal.

- *Step 4:* The above signal and E_{02} are constructed to E_0 by Eq. 35. In addition, transform it by the inverse DCRT,

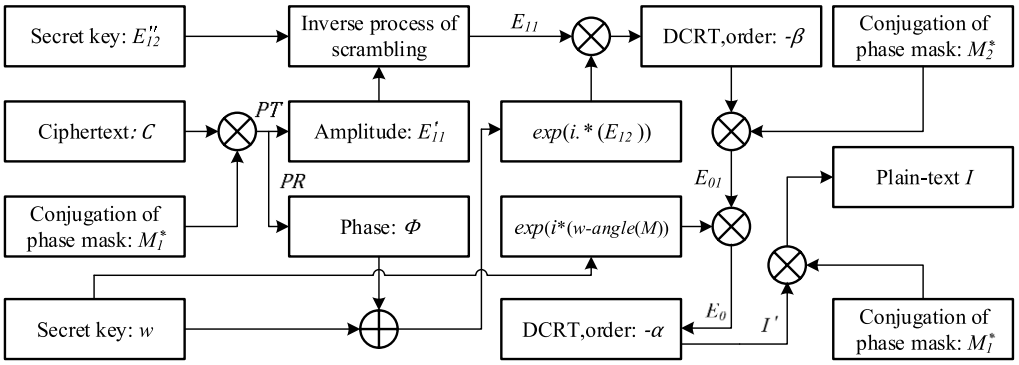

FIGURE 4. Diagram of decryption scheme.

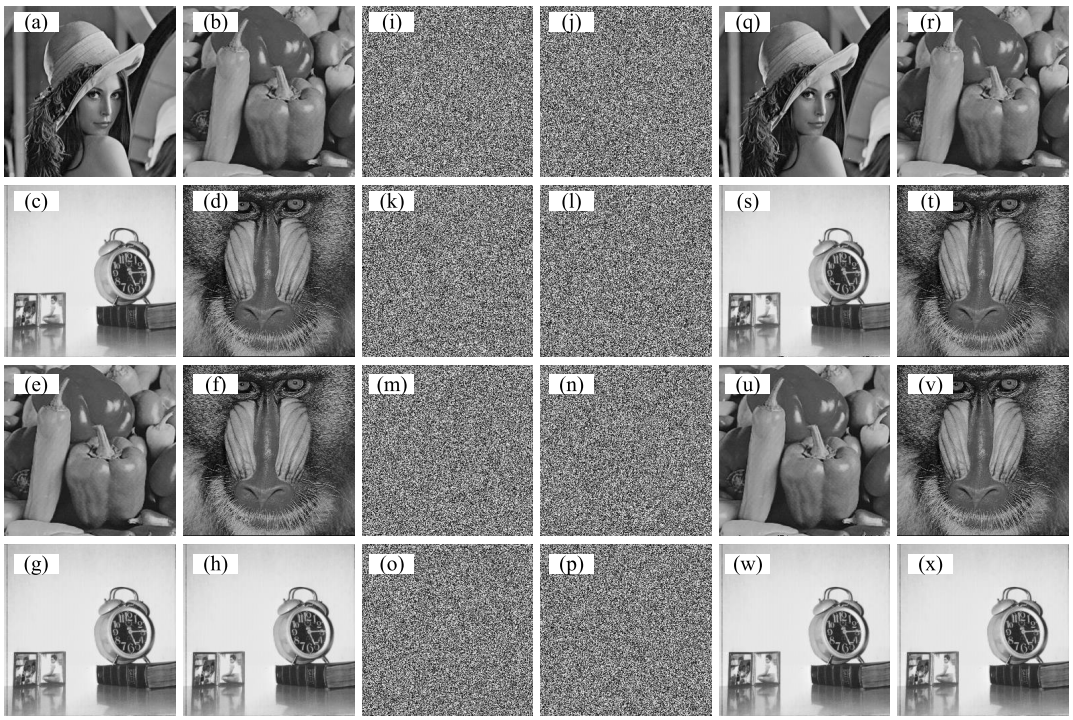

FIGURE 5. The simulation results of the encryption and decryption: (a)-(h) are four pair of plaintext images; (i)-(p) are the corresponding encrypted images of (a)-(h); and (q)-(x) are the decrypted images with right keys.

the detailed formula is

$$\begin{cases} E_0 = E_{01} \cdot exp(1i * E_{02}) \\ I' = R^{-\alpha} * E_0. \end{cases} \tag{35}$$

- *Step 5:* Utilize M_1^* to multiply I' number-by-number:

$$I = I' \cdot M_1^*. \tag{36}$$

- *Step 6:* The plain-text I is divided into phase decrypted image I_2 and amplitude decrypted image I_1:

$$\begin{cases} I_1 = abs(I) \\ I_2 = angle(I)/\pi. \end{cases} \tag{37}$$

C. EXPERIMENTAL RESULTS

Several grey images with the size of 256 × 256 are experimented in the numerical simulations. All the tests are operated under the MATLAB R2014a platform on a Windows10 operating system with 8GB RAM, a 2.80 GHz processor, and Intel(R) Core(TM) i7-7700HQ. The control parameters of the Chen system are $a = 35$, $b = 3$, and $c = 28$, and its initial parameters are generated by self-adapting parameter σ_{adinit}. Then the initial values of 2D Logistic maps are $x'_0 = 0.0924 + 0.01\sigma_{adinit}$, and $y'_0 = 0.9564 + 0.01\sigma_{adinit}$ and the control parameters are $r_1 = 0.19$, $r_2 = 0.14$, $\mu_1 = 3.0231$, and $\mu_2 = 2.9974$. Eventually, the orders of DCRT are set to be $\alpha = means(I)$, and $\beta = 0.565623 + 0.65865i - 0.01\sigma_{adinit} + 0.01\sigma_{adinit} * i$, and the coefficients $\varepsilon = 0.2525$.

The experimental results are shown in Fig. 5 in which Fig. 5(a)-(h) are plain-images, and these images are in pairs to be encrypted, such as (a) and (b), (c) and (d), (e) and (f), (g) and (h). In these pairs of images, the image on the left is used as the phase and the image on the right is used as

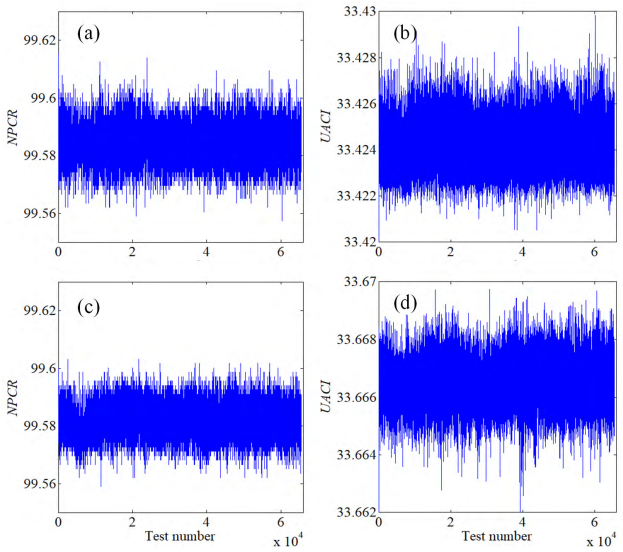

FIGURE 6. Test of *NPCR* and *UACI*: (a) and (b) are the *NPCR* and *UACI* curve of the amplitude encrypted graph; (c) and (d) are the *NPCR* and *UACI* curve of the phase encrypted graph.

the amplitude of Eq. 21. Fig. 5(i)-(p) are the corresponding cipher-images of Figure 5(a)-(h), and the corrected decrypted images are Fig. 5 (q)-(x).

IV. PERFORMANCE ANALYSIS AND DISCUSSION

A. DIFFERENTIAL ATTACK ANALYSIS

The ability to resist the differential attack (DA) is an important indicator to assess the performance of the algorithm. Specifically, a good encryption scheme should make the cipher-image have huge difference from each other only if the corresponding plaintext have one-bit change. In general, the number of pixel's change rate (*NPCR*) and the unified averaged changing intensity (*UACI*) are used to test the capability to withstand differential attack, and they are defined by

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{38}$$

$$UACI = \frac{1}{MN}[\sum_{i,j} \frac{|P_1(i,j) - P_2(i,j)|}{255}] \times 100\%. \tag{39}$$

Suppose the size of the plain-image is $M \times N$, and P_1 is the encrypted image of the plain-image I_1, and P_2 is the cipher-image of the plain-image I_2 which only has one-bit difference from the plain-text I_1. Moreover $D(i,j)$ is defined by

$$D(i,j) = \begin{cases} 0, & P_1(i,j) = P_2(i,j) \\ 1, & P_1(i,j) \neq P_2(i,j). \end{cases} \tag{40}$$

Taking the "Peppers" and "Lena" with size of 256 × 256 as the example, each pixel's lowest bit of each position is changed successively, and get the corresponding cipher-images. The experimental *NPCR* and *UACI* results at different locations of amplitude encrypted image and phase encrypted image are shown in Fig. 6.

As shown in the following chart, there is a great difference between the encrypted images even though a slight change exists in the plain-images. Specifically, the average values of *NPCR* and *UACI* about the amplitude cipher-image are 99.5838% and 33.4242% and the mean values of *NPCR* and *UACI* about the phase encrypted image approach 99.5815% and 33.6665%. Then, compare the *NPCR* and *UACI* about the phase encrypted image to the other related papers shown in Table 1, it can be seen that the encryption scheme has a good capacity to resist DA.

TABLE 1. The *NPCR* and *UACI* of encrypted image "Lena" in different methods.

$''Lena''$	$NPCR(\%)$	$UACI(\%)$
Ref. [39]	99.4746%	33.3774%
Ref. [40]	99.4602%	33.6389%
Ref. [16]	99.60%	33.47%
Ref. [41]	99.5956%	33.5512%
Ref. [42]	99.59%	33.45%
Proposed algorithm	99.5815%	33.6665%

B. KEY SPACE ANALYSIS

The secret key of this encryption scheme is divided into two classes, phase keys (key_1, key_2) and external keys of (i) two initial values (x_0', y_0') of the 2D Logistic maps, and the order of DCRT (β), and (ii) two control parameters (μ_1, μ_2) of the 2D Logistic maps and the coefficients ε in Eq. 8. If the computing precision is 10^{-15}, the size of the key space is 10^{75} according to the external keys, which is larger than 2^{128} [4] and can effectively resist brute-force attacks [17].

As for the phase keys (key_1, key_2), as shown in Fig. 7, the $max(\Delta d) \approx 0.025$. As d is used to control the range of phase by Eq. 43, the effective range of d is 2π. Therefore, the number of each point in the phase key can be estimated to be $2\pi/0.025 \approx 251$. Therefore, if the size of the plain-image is supposed to be $N \times N$, the possible space of the phase key can be $251^{N\times N}$ because it is related to the size of the plain-image. Considering the existence of two phase keys, the total key space is $(10^{75} + 2 \times 251^{N\times N}) > 2^{128}$, which is enough to resist the violent attacks [28].

C. KEY SENSITIVITY ANALYSIS

Key sensitivity is an important index to measure the performance of encryption algorithm, which includes the external key sensitivity analysis and the phase key sensitivity analysis.

1) THE EXTERNAL KEY SENSITIVITY ANALYSIS

Only use a wrong external secret key to decrypt the original encrypted image, and observe the difference between the original image and the decrypted image. Generally, mean square error (*MSE*) and peak signal-to-noise ratio (*PSNR*) are two common criterion to measure this difference [16], which are expressed by

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} [D(x,y) - P(x,y)]^2, \tag{41}$$

$$PSNR = 10log_{10} \frac{255 \times 255}{MSE}, \tag{42}$$

TABLE 2. Key sensitivity about double-image encryption with slight changes of the external keys.

The wrong keys		$NPCR(\%)$	$UACI(\%)$	MSE	$PSNR$
$x_0'' = x_0' + 10^{-14}$	Amplitude	99.4141	21.7502	4710.7271	11.3999
	Phase	99.8062	34.5162	10700.9569	7.8366
$y_0'' = y_0' + 10^{-14}$	Amplitude	99.4156	22.8577	4741.0633	11.3720
	Phase	99.8016	34.2585	10557.4656	7.8952
$\beta' = \beta + 0.01$	Amplitude	99.4278	21.3895	4569.4426	11.5322
	Phase	99.8032	32.5414	9703.0331	8.2617
$\beta'' + 0.01i$	Amplitude	99.3698	20.6626	4273.3825	11.8231
	Phase	99.8352	37.9511	12395.5385	7.1981

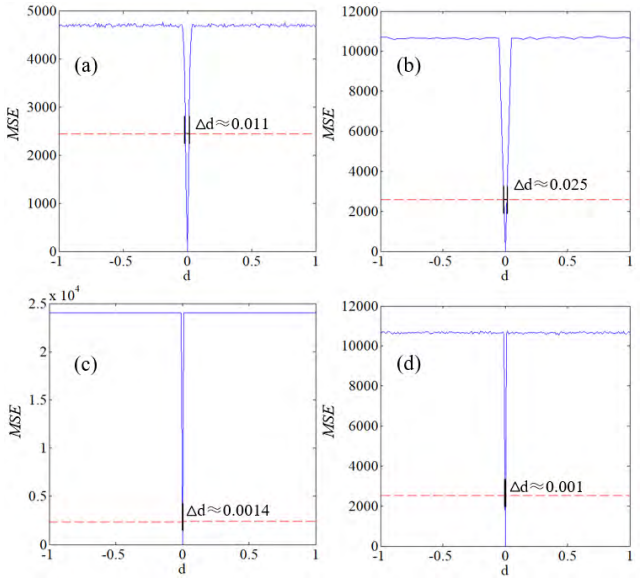

FIGURE 7. The *MSE* curves: (a) and (b) are the *MSE* curve of amplitude decryption and phase decryption image by using the pseudo key key_1' with different parameters d; (c) and (d) are the *MSE* curve of amplitude decryption and phase decryption image by using the pseudo key key_2' with different parameters d.

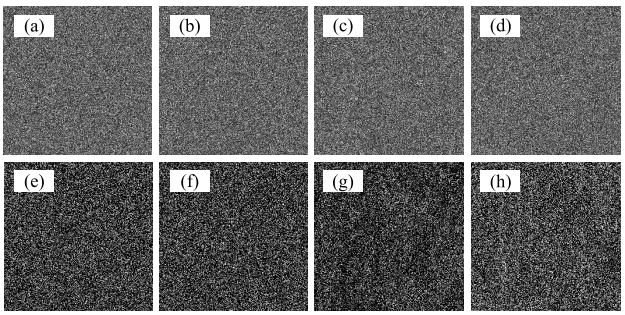

FIGURE 8. The decrypted images with the wrong keys: (a) and (e) are the amplitude decrypted image and phase decrypted image with the wrong key $x_0'' = x_0' + 10^{-14}$; (b) and (f) are the amplitude decrypted image and phase decrypted image with the wrong key $y_0'' = y_0' + 10^{-14}$; (c) and (g) are the amplitude decrypted image and phase decrypted image with the wrong key $\beta' = \beta + 0.01$; (d) and (h) are the amplitude decrypted image and phase decrypted image with the wrong key $\beta'' = \beta + 0.01i$.

where D is a decrypted image with the wrong secret keys and P is plain-image. Fig. 8 shows the wrong decrypted results for the original images in Fig. 5(a) and (b), in which Fig. 8(a)-(d) are the amplitude decrypted images and Fig. 8(e)- (h) are the phase decrypted images when external keys x_0', y_0', and β have a slight change, respectively. From Fig. 8, it can be seen that the decrypted images are greatly different from the plain-text "Lena" and "Peppers". Besides, the curves of the *MSE* is drawn in Fig. 9, and the result of numerical analysis on the external keys sensitivity is listed in Table 2. From the Fig. 9 and Table 2, we can see that the proposed double-image encryption scheme is high sensitivity for external secret keys.

2) THE PHASE KEY SENSITIVITY ANALYSIS

Except for the external keys, the sensitivity to the phase key is also very critical to resist the blind encryption attack. Suppose all the external keys and encryption scheme are known except for the phase keys [28], then two close pseudo keys are used to decrypt, which can be described by

$$\begin{cases} key_1' = key_1 + d * \Delta key \\ key_2' = key_2 + d * \Delta key, \end{cases} \tag{43}$$

where Δkey is a random function with a range of $[-1, 1]$, and d is a coefficient be used to control the interference intensity. The key_1' and key_2' are separately used to decrypt, and then the corresponding *MSE* curves of the amplitude decrypted image and phase decrypted image can be gained and drawn in Fig. 7.

In Fig. 7, the red dotted line is a threshold mark, *MSE*=2500 at that point. Δd is the distance between the left and the right of coefficients d when it reaches the threshold. If the *MSE* value is less than the value of the threshold, it will be considered that a small amount of information of the original image can be reconstructed. Fig. 7 show that even though there is a slight deviation from the correct key, the value of *MSE* will still be very large. Therefore, it can be concluded that the proposed scheme is highly sensitive to the phase key which make it difficult for attackers to get the correct keys.

D. STATISTICAL ANALYSIS

1) THE HISTOGRAM ANALYSIS

The histogram of the image exhibits the distribution of the pixels of image and reflects the statistical feature of the image

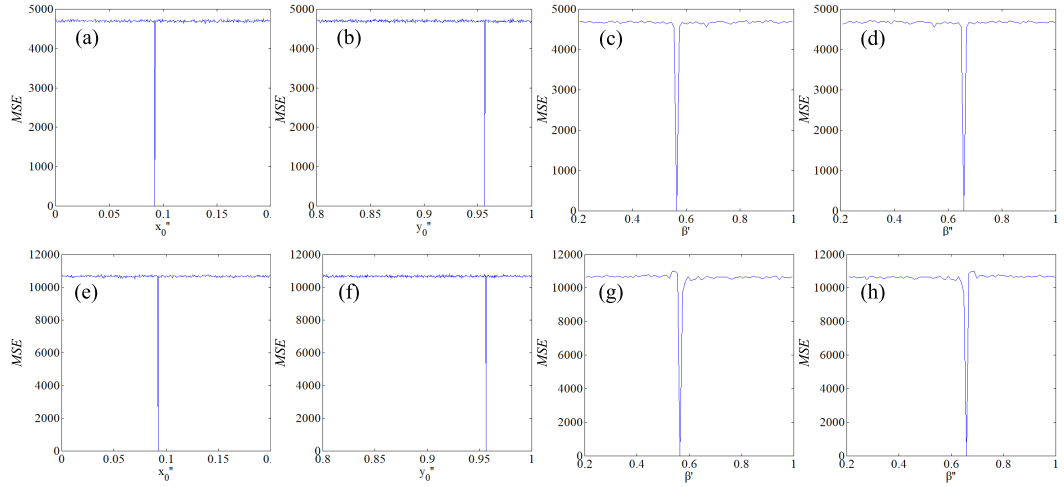

FIGURE 9. The curves of *MSE*: (a) and (e) are the *MSE* curves of the amplitude decrypted image and phase decrypted image with wrong key x_0'; (b) and (f) are the *MSE* curves of the amplitude decrypted image and phase decrypted image with wrong key y_0'; (c) and (g) are the *MSE* curves of the amplitude decrypted image and phase decrypted image with wrong key β'; (d) and (h) are the *MSE* curves of the amplitude decrypted image and phase decrypted image with wrong key β''.

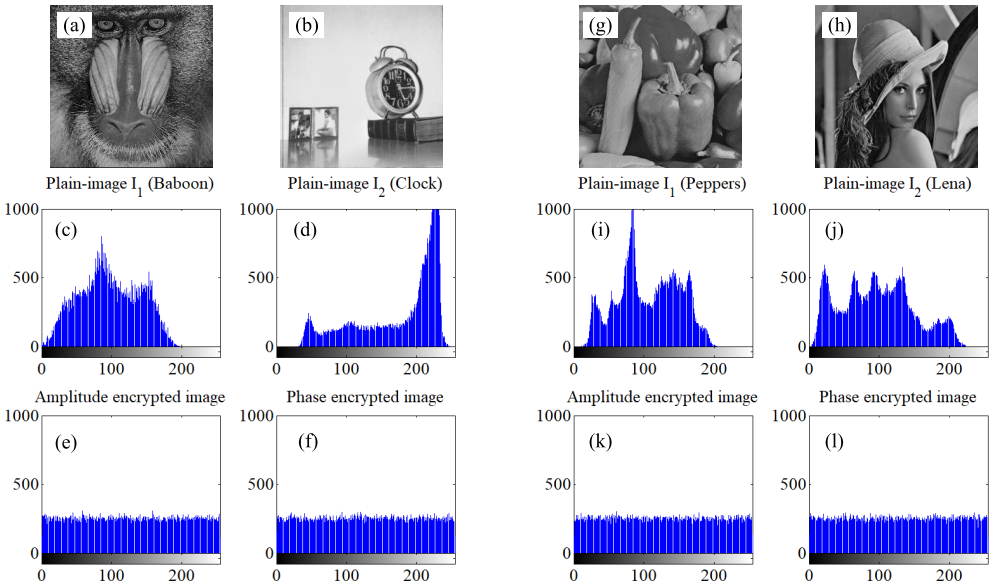

FIGURE 10. Histograms: (a), (b) and (g), (h) are original images; (c), (d) and (i), (j) are the histograms of original histograms; (e) and (f) are the histograms of the encrypted images of (a) and (b); (k) and (l) are the histograms of the encrypted images of (g) and (h).

to some extent. Therefore, to effectively resist the statistical attack, the histogram of the encrypted images must be guaranteed smooth and evenly distributed [43]. The histograms of this work are shown in Fig. 10, in which Fig. 10 (a), (b), (g) and (h) are the original images, (c), (d), (i), and (j) are the corresponding histograms of the original images, and (e), (f), (k), and (l) are the corresponding histograms of the encrypted images. From Fig. 10, it can be seen the distribution characteristics of plain-images can be seen clearly, but the distribution information of pixels about the encrypted image is very uniform.

2) CORRELATION-COEFFICIENT ANALYSIS

The original image contains a large number of redundant information, which is shown to be a strong correlation between adjacent pixels in all directions, the strong correlation is an important message for decipher to crack the cipher-text. Therefore the correlation coefficient cor_{xy} between adjacent pixels of cipher-images in all directions is a criterion to measure the performance of an encryption system, and cor_{xy} can be denoted by

$$cor_{xy} = \frac{E((x_i - E(x))(y_i - E(y)))}{\sqrt{D(x)D(y)}}, \tag{44}$$

TABLE 3. Correlation coefficient between the adjacent pixels of images.

Image	Horizontal direction	Vertical direction	diagonal direction
"Peppers"	0.9656	0.9724	0.9414
"Lena"	0.9407	0.9695	0.9227
Amplitude encrypted image in this work	-0.0018	0.0031	9.8031-e04
Phase encrypted image in this work	-0.0014	0.0028	-1.6877e-04

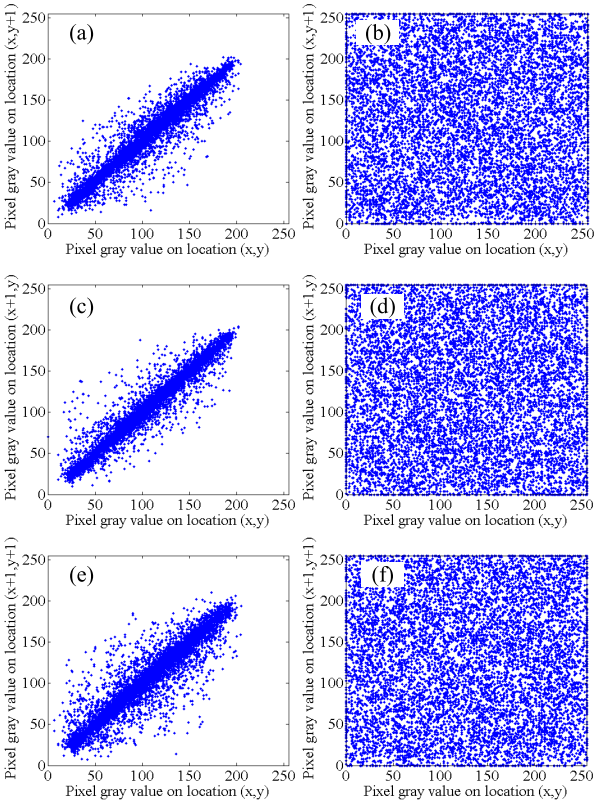

FIGURE 11. Correlation distribution of the plain-image I_1 "Peppers" and the amplitude encrypted image: (a) the horizontal correlation distribution of I_1; (b) the horizontal correlation distribution of the amplitude encrypted image; (c) the vertical correlation distribution of I_1; (d) the vertical correlation distribution of the amplitude encrypted image; (e) the diagonal correlation distribution of I_1; (f) the diagonal correlation distribution of the amplitude encrypted image.

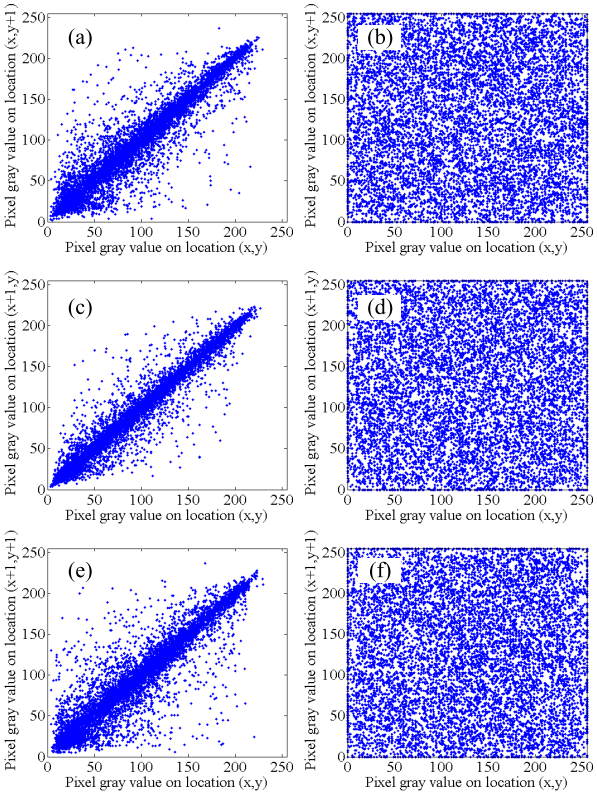

FIGURE 12. Correlation distribution of the plain-image I_2 "Lena" and the phase encrypted image: (a) the horizontal correlation distribution of I_2; (b) the horizontal correlation distribution of the phase encrypted image; (c) the vertical correlation distribution of I_2; (d) the vertical correlation distribution of the phase encrypted image; (e) the diagonal correlation distribution of I_2; (f) the diagonal correlation distribution of the phase encrypted image.

where $E(X) = \frac{1}{N}\sum_{i=1}^{N} x_i$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$, x and y represent the pixel values of the adjacent positions of the image, respectively. Moreover, N is the number of the adjacent pixels of the image. Firstly, 10000 pairs of adjacent pixels of the original image "Peppers" and "Lena" and the amplitude/phase encrypted images are chosen to plot, and the result is shown in Fig. 11 and Fig. 12. From these figures, it can be seen there is a high correlation between the adjacent pixels of the original image in three direction. However, the correlation between the adjacent pixels is broken for the amplitude encrypted image and phase encrypted image in three direction.

Secondly, the correlation coefficient cor_{xy} between adjacent pixels of images are calculated in terms of Eq. 44, and the result is listed in Table 3. The experimental data illustrates that the correlation coefficient cor_{xy} of the amplitude/phase encrypted images is close to 0 which shows the proposed double-image encryption scheme has strong resistance to statistical attacks.

E. OCCLUSION AND NOISE ATTACK ANALYSIS

In the process of information transmission, noise and congestion are unavoidable once network failure occurs [4]. Therefore, it is also critical to resist the occlusion attack and noise attack for the encryption scheme.

1) OCCLUSION ATTACK ANALYSIS

In the experiment of occlusion attack analysis, four images are taken as one group and the different groups represent different occlusion attack analysis. For a group, the first

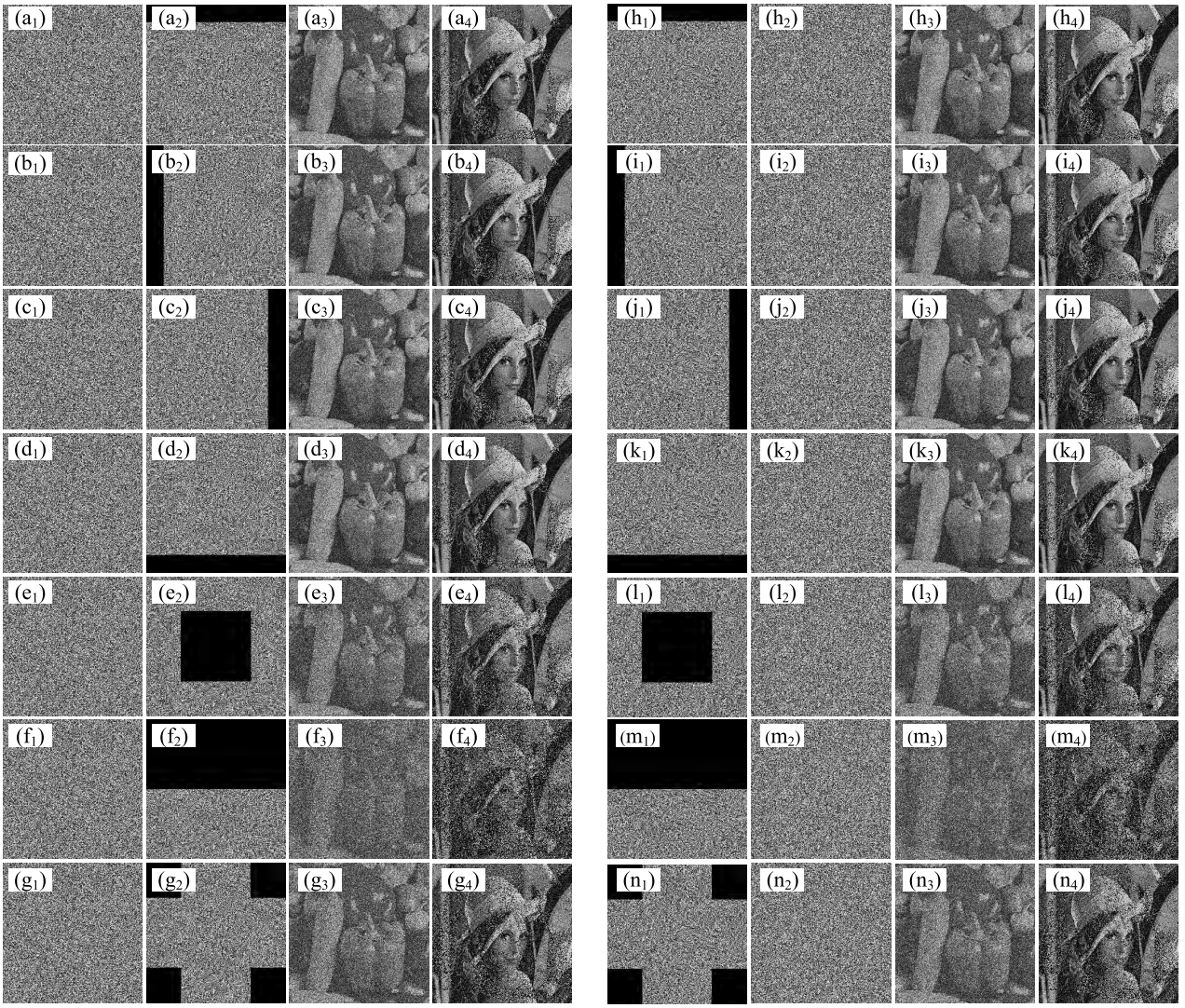

FIGURE 13. Occlusion attack analysis, (a_2), (b_2), (c_2), (d_2): phase cipher-image with 12.5% occlusion; (h_1), (i_1), (j_1), (k_1): amplitude cipher-image with 12.5% occlusion; (e_2), (g_2): phase cipher-image with 25% occlusion; (l_1), (n_1): amplitude cipher-image with 25% occlusion; (f_2): phase cipher-image with 50% occlusion; (m_1): amplitude cipher-image with 50% occlusion; (a_3)-(g_3), (a_4)-(g_4), (h_3)-(n_3), (h_4)-(n_4): decrypted images of the corresponding group.

and second images are amplitude encrypted image and phase encrypted image, and the latter two are the corresponding decrypted images. In this experiment, 14 groups are used, and the encrypted images and decrypted images in the same group are distinguished by subscript, such as group (a_1), (a_2), (a_3), (a_4) and so on.

As shown in the Figure 13, after executing different degree of occlusion attack, the decrypted images can still be identified, thus it denotes the encryption scheme has a certain resistance to different degrees of occlusion attack in different locations.

2) NOISE ANALYSIS

Gaussian random noise and Salt-and-pepper noise are used to test the ability of resisting noise attacks. The Gaussian noise is added to the cipher-text C that is from Eq. 21 by

$$C' = C + kG, \tag{45}$$

where C' is new encryption synthetic signal, k is noise intensities and G is the standard Gaussian noise data with zero-mean and standard deviation of 1. The decrypted image of ''Peppers'' and ''Lena'' after adding Gaussian noise and corresponding *MSE* curve with a different k are shown in Figure 14. Moreover, from Fig. 14(a)-(h), it can be seen that the decrypted images can still be identified at $k = 30$. Thus, the double images encryption scheme in this paper has a stronger resistance to Gauss noise attack.

In this test, Fig.15 and Table 4 exhibit the test results in the case of different noise density of Salt-and-pepper noise. As shown above, the decrypted images in the case of Salt-and-pepper noise can still be recognized, furthermore, there is a lower *MSE* value of the decrypted image in this propose scheme than that in [35]. Therefore, it can be seen that this encryption system has a stronger resistance to Salt-and-pepper noise attacks.

TABLE 4. ***MSE*** **performance about Salt-and-peppers noise attack.**

Salt-and-peppers noise	0.1%	0.5%	1.0%	5.0%
(Ref. [35])Decrypted "Peppers"	29.7694	145.0776	289.1082	1397.1740
(Ref. [35])Decrypted "Lena"	38.1496	231.2067	437.1599	1660.8500
Decrypted "Peppers"	2.4561e-04	9.2312e-04	0.0018	0.0096
Decrypted "Lena"	4.3041e-04	0.0019	0.0049	0.0335

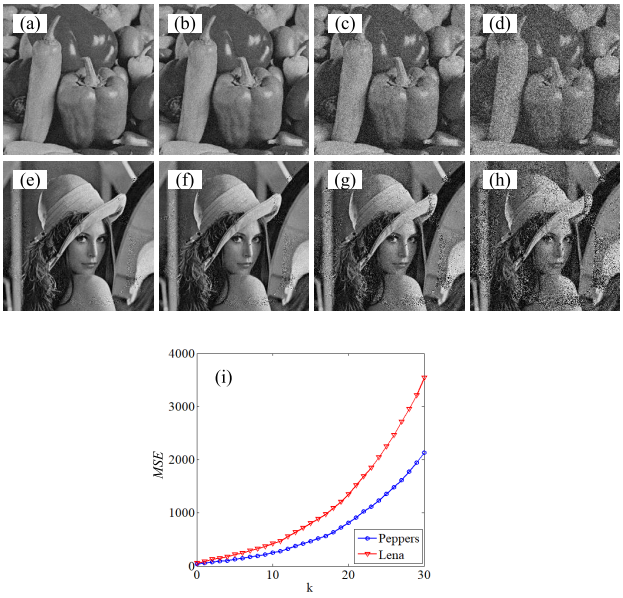

FIGURE 14. **Decrypted images and the corresponding *MSE* curve in different Gaussian white noise intensities k: (a), (e):$k = 5$; (b), (f): $k = 10$; (c), (g): $k = 20$; (d), (h): $k = 30$, and (i) *MSE* curve about noise intensities k.**

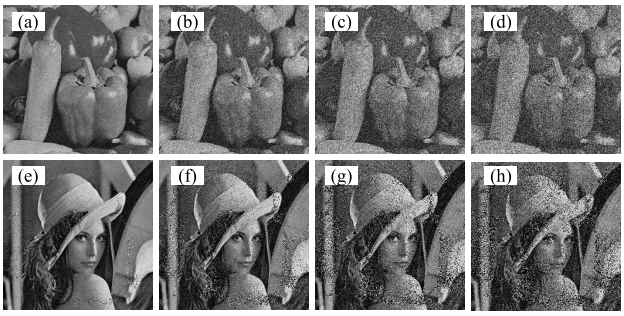

FIGURE 15. **Salt-and-pepper noise attack analysis, the decrypted images after adding Salt-and-pepper noise of density (a), (e): 1%; (b), (f): 5%; (c), (g): 10%; (d),(h): 15%.**

F. SPEED ANALYSIS AND COMPARISIONS

The encryption algorithm should not only have good encryption effect, but also have a certain requirement in speed. In this work, the proposed scheme can be divided into three parts: encryption process, decryption process, reading and displaying encrypted and decrypted images. Specifically, the encryption process contains the generation of the chaotic sequences, the phase mask generation, the transform matrix construction, and the encryption algorithm execution.

Taking the images "Peppers" and "Lena" with the size of 256 × 256 as the examples, the experiment is executed for 20 times, and the average time of encryption process is 0.0748s. The executing time of each part of the total algorithm is shown in Fig. 16. The total required time is 0.4637s where the encryption process needs 0.0748s and reading and displaying images takes the longest time of 0.366s.

TABLE 5. **Speed analysis and comparisons.**

Encryption process of the proposed algorithm	Ref. [44]	Ref. [4]	Ref. [39]	Ref. [45]
0.0748s	0.613s	1.6706s	0.113s	0.719s

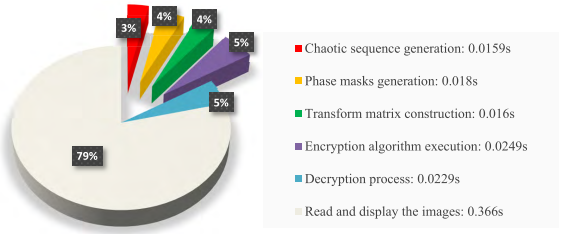

FIGURE 16. **The speed analysis of proposed algorithm for "Peppers" and "Lena" with size of 256 × 256.**

This work is compared with other approaches and the results are shown in Table 5. As shown in Fig. 16 and Table 5, the total execution time of this algorithm in this work is 0.4637s, and the average time of the encryption process is 0.0748s. Compared with the speed in [4], [39], [44], and [45], the speed of encryption process in this work is the best. Besides, this proposed scheme can simultaneously encrypt two images, i.e., "Lena" and "Peppers", which further illustrates the superiority of the double-image encryption scheme.

V. CONCLUSIONS

In this work, a novel double-image encryption scheme is proposed, which combines amplitude-phase encoding with DCRT (due to its stronger randomness and better degree of freedom about the key generations than DFrRT). Specifically, the self-adapting parameter and phase masks are utilized to improve the capability of resisting differential attacks. The experimental results and numerical simulation show that the proposed encryption scheme has good key sensitivity, fast execution speed, a uniform distribution of histogram for encrypted images which can effectively resist violent and statistical attacks, and good robustness under the noise, occlusion and differential attacks. Therefore the proposed encryption scheme can potentially be used in multimedia data security applications.

REFERENCES

[1] J. S. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 3, pp. 578–588, 2014.
[2] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.
[3] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, 2011.
[4] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, and J. Liu, "A chaotic map-control-based and the plain image-related cryptosystem," *Nonlinear Dyn*, vol. 83, no. 4, pp. 2293–2310, 2015.
[5] X. Chai, K. Yang, and Z. Gan, "A new chaos-based image encryption algorithm with dynamic key selection mechanisms," *Multimedia Tools, Appl.*, vol. 76, no. 7, pp. 9907–9927, 2017.
[6] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, 2017.
[7] X. Wang, C. Liu, and D. Xu, "Image encryption scheme using chaos and simulated annealing algorithm," *Nonlinear Dyn.*, vol. 84, no. 3, pp. 1417–1429, 2016.
[8] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.
[9] W. Xingyuan, F. Le, W. Shibing, C. Zhang, and Z. Yingqian, "Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption," *IEEE Access*, vol. 6, pp. 39705–39724, 2018.
[10] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tool, Appl.*, vol. 76, no. 5, pp. 6229–6245, 2017.
[11] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, 2016.
[12] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 51–66, 2017.
[13] F. Özkaynak and A. B. Özer, "Cryptanalysis of a new image encryption algorithm based on chaos," *Optik Int. J. Light Electron Opt.*, vol. 127, no. 13, pp. 5190–5192, 2016.
[14] L. Gong, C. Deng, S. Pan, and N. Zhou, "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," *Opt. Laser Technol.*, vol. 103, no. 1, pp. 48–58, 2018.
[15] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018.
[16] X.-L. Chai, Z.-H. Gan, K. Yuan, Y. Lu, and Y.-R. Chen, "An image encryption scheme based on three-dimensional Brownian motion and chaotic system," *Chin. Phys. B*, vol. 26, no. 2, pp. 99–113, 2017.
[17] Y.-L. Luo, R.-L. Zhou, J.-X. Liu, S.-H. Qiu, and Y. Cao, "A novel image encryption scheme based on Kepler's third law and random Hadamard transform," *Chin. Phys. B*, vol. 26, no. 12, pp. 1–14, 2017.
[18] H. T. Chang and M. Spie, "Image encryption using separable amplitude-based virtual image and iteratively retrieved phase information," *Opt. Eng.*, vol. 40, no. 10, pp. 2165–2171, 2001.
[19] I. S. I. Abuhaiba and M. A. S. Hassan, "Image encryption using differential evolution approach in frequency domain," *Signal, Image Process.*, vol. 2, no. 1, pp. 51–69, 2011.
[20] Q. Wang, D. Xiong, A. Alfalou, and C. Brosseau, "Optical image encryption method based on incoherent imaging and polarized light encoding," *Opt. Commun.*, vol. 415, no. 1, pp. 56–63, 2018.
[21] B. Hennelly and J. Sheridan, "Image encryption and the fractional Fourier transform," *Optik*, vol. 114, no. 6, pp. 251–265, 2003.
[22] C. Jimenez, C. Torres, and L. Mattos, "Fractional Hartley transform applied to optical image encryption," *J. Phys., Conf. Ser.*, vol. 274, no. 1, pp. 12041–12046, 2011.
[23] Z. Liu *et al.*, "Image encryption algorithm based on the random local phase encoding in gyrator transform domains," *Opt. Commun.*, vol. 285, no. 19, pp. 3921–3925, 2012.
[24] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Security analysis of optical encryption," *Proc. SPIE*, vol. 5986, no. 1, pp. 25–34, Oct. 2005.
[25] N. Zhou, J. Yang, C. Tan, S. Pan, and Z. Zhou, "Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform," *Opt. Commun.*, vol. 354, pp. 112–121, Nov. 2015.
[26] N. Singh and A. Sinha, "Optical image encryption using improper Hartley transforms and chaos," *Optik*, vol. 121, no. 10, pp. 918–925, 2010.
[27] J. M. Vilardy, C. J. Jimenez, and R. Perez, "Image encryption using the Gyrator transform and random phase masks generated by using chaos," *J. Phys., Conf. Ser.*, vol. 850, no. 1, p. 012012, 2017.
[28] Z. Liu, J. Dai, X. Sun, and S. Liu, "Triple image encryption scheme in fractional Fourier transform domains," *Opt. Commun.*, vol. 282, no. 4, pp. 518–522, 2009.
[29] X. Wang and D. Zhao, "Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain," *Opt. Commun.*, vol. 284, no. 1, pp. 148–152, 2011.
[30] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and permutation," *Opt. Lasers Eng.*, vol. 92, no. 1, pp. 6–16, 2017.
[31] H. Li, Y. Wang, H. Yan, L. Li, Q. Li, and X. Zhao, "Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform," *Opt. Lasers Eng.*, vol. 51, no. 12, pp. 1327–1331, 2013.
[32] H. Zhao, Z. Zhong, W. Fang, H. Xie, Y. Zhang, and M. Shan, "Double-image encryption using chaotic maps and nonlinear non-DC joint fractional Fourier transform correlator," *Opt. Eng.*, vol. 55, no. 9, p. 093109, 2017.
[33] F. Han, X. Liao, H. Wang, B. Yang, and Y. Zhang, "A self-adaptive scheme for double color-image encryption," in *Proc. 9th Int. Conf. Adv. Comput. Intell. (ICACI)*, 2017, pp. 121–128, no. 1.
[34] F. Han, X. Liao, B. Yang, and Y. Zhang, "A hybrid scheme for self-adaptive double color-image encryption," *Multimedia Tools, Appl.*, vol. 77, no. 11, pp. 14285–14304, 2018.
[35] Y. Zhang and D. Xiao, "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform," *Opt. Lasers Eng.*, vol. 51, no. 4, pp. 472–480, Apr. 2013.
[36] L. Sui, H. Lu, Z. Wang, and Q. Sun, "Double-image encryption using discrete fractional random transform and logistic maps," *Opt. Lasers Eng.*, vol. 56, no. 5, pp. 1–12, 2014.
[37] C. Li and G. Peng, "Chaos in Chen's system with a fractional order," *Chaos Solitons, Fractals*, vol. 22, no. 2, pp. 443–450, 2004.
[38] T. Zhou, Y. Tang, and G. Chen, "Complex dynamical behaviors of the chaotic Chen's system," *Int. J.*, vol. 13, no. 9, pp. 2561–2574, 2003.
[39] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 447–460, 2015.
[40] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 665–673, 2013.
[41] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Opt. Lasers Eng.*, vol. 107, no. 1, pp. 370–379, 2018.
[42] C. Fu, Z. Wen, Z. Zhu, and H. Yu, "A security improved image encryption scheme based on chaotic Baker map and hyperchaotic Lorenz system," *Int. J. Comput. Sci., Eng.*, vol. 12, nos. 2–3, pp. 113–123, 2016.
[43] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
[44] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Opt. Lasers Eng.*, vol. 91, no. 1, pp. 41–52, 2017.
[45] X. Zhang, G. Zhu, and S. Ma, "Remote-sensing image encryption in hybrid domains," *Opt. Commun.*, vol. 285, no. 7, pp. 1736–1743, 2012.

YULING LUO received the Ph.D. degree in information and communication engineering from the South China University of Technology, Guangzhou, China. She is currently an Associate Professor with the Faculty of Electronic Engineering, Guangxi Normal University, Guilin, China. Her research interests include information security, image processing, chaos theory, and embedded system implementations.

SHUNBIN TANG received the B.E. degree from the Tianjin University of Technology and Education, China, in 2017. He is currently pursuing the master's degree with the Faculty of Electronic Engineering, Guangxi Normal University. His research interests include information security, multimedia data encryption, and its application.

XINGSHENG QIN received the B.S. degree in optical information science and technology from the Guilin University of Electronic Technology and the M.S. degree in measuring and testing technologies and instruments from the University of Shanghai for Science and Technology. His research interests include information security, embedded system, and its application.

LVCHEN CAO received the B.Eng. degree in electronic and information engineering from the Zhongyuan University of Technology, Zhengzhou, China, in 2013, and the M.S. degree in electronic science and technology from Guangxi Normal University, Guilin, China, in 2016. He is currently pursuing the Ph.D. degree with the Beijing Institute of Technology. He was an Algorithm Engineer with ALi Corporation, Zhuhai, China, from 2016 to 2017. His current research interests include pattern recognition, machine learning, and chaotic cryptography.

FRANK JIANG received the Ph.D. degree from the University of Technology Sydney in 2008 and the master's degree in computer science from the University of New South Wales (UNSW). He gained the 3.5 years of post-doctoral research experience at UNSW. He has published over 80 highly reputed SCI/EI indexed journals and conferences articles. His main research interests include biologically inspired learning schemes and their applications in the context-aware systems, data-driven cyber security, predictive analytics, and blockchain techniques.

JUNXIU LIU, photograph and biography not available at the time of publication.