IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 10, 2019, accepted July 17, 2019, date of publication July 24, 2019, date of current version August 29, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2930183*

# Homogenized Chebyshev-Arnold Map and Its Application to Color Image Encryption

**XUEJING KANG[1], (Member, IEEE), XUANSHU LUO[1], XUESONG ZHANG[1], (Member, IEEE), AND JING JIANG[2]**

[1]School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]Department of Communication Engineering, Beijing Union University, Beijing 100101, China

Corresponding author: Jing Jiang (xxtjiangjing@buu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61701036 and Grant 61871055, in part by the Fundamental Research Funds for the New Start Plan Project of Beijing Union University under Grant Zk10201604, and in part by the Fundamental Research Funds for the Central Universities under Grant 2018RC54.

**ABSTRACT** In this paper, we propose a homogenized Chebyshev-Arnold map (HCAM) by homogenizing the linear coupling of Chebyshev map and Arnold map. The proposed HCAM has complex dynamical behaviors and can avoid the problems of the original Chebyshev map when used in image encryption. Based on the HCAM, we present a color image encryption algorithm that contains confusion and diffusion processes. In the confusion stage, we use the random chaotic matrix transform (RCMT) to randomize the shifting steps, which can eliminate the regular pattern of the original CMT and enhance the security level. In the diffusion stage, we use a SHA-512- and SHA-384-based fast pixel substitution scheme to perform the bit-level exclusive-or operation, which can obtain outstanding self-adaptiveness and high efficiency. The experimental results and security analysis demonstrate that the proposed algorithm has high level of security and robust to the potential attacks.

**INDEX TERMS** Color image encryption, Chebyshev map, Arnold Map, chaotic matrix transform, secure hash algorithm.

## I. INTRODUCTION

With the rapid growth of digital technique and modern communication, a large amount of digital data have been generated and spread on public channels. Since digital images contain rich information and can visually present the scene, they are widely transmitting on the Internet and bring the security problem for some confidential or private images (such as the military images, telemedicine images, and personal images). The conventional textual encryption techniques, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [1], are not secure enough to protect image data due to their high correlation and redundancy among adjacent pixels. Therefore, it is urgent to propose efficient techniques to protect the digital images travelling on public channels.

Since image encryption is the most straightforward way for image protection, it becomes the hotspot of cryptography in recent years [2]–[6]. Among them, the chaos-based encryptions have excellent performance because the chaotic systems have the properties of ergodicity, deterministic dynamics and sensitivity to the initialize conditions. Therefore, various chaos-based encryption schemes have been developed [7]–[25]. For example, Wang proposed image encryption methods by using dynamic random growth technique [7], one-time keys [8], bit-level permutation [9], the perceptron model [10] and parallel computing system [12]. Zhang [13] proposed a fast image cryptosystem by employing chaotic map and cubic S-box. Ma *et al.* [14] designed a plaintext-related scheme to improve the ability of chaos-based methods against plaintext attack. Zahmoul *et al.* [18] created a new chaotic map based on Beta function and apply it to image encryption with high efficiency. Hua *et al.* [19] combined a two-dimensional Sine Logistic Modulation Map (2D-SLMM) and a chaotic magic transform (CMT) for image encryption with low time complexity. Among various chaotic systems, the Chebyshev map [21] is widely employed for image encryption due to its extremely large range of control parameter. For instance, Fu *et al.* [22] used Chebyshev map to process the diffusion

The associate editor coordinating the review of this manuscript and approving it for publication was Shubhajit Roy Chowdhury.

part as a key stream generator and gained high security level. Stoyanov and Kordov [23] obtained pseudorandom bit with the help of Chebyshev map and used them for image encryption. Wang *et al.* [24] proposed a two-dimensional cross chaotic map based on Chebyshev map to reduce the calculation complexity and obtain high encryption efficiency. Ramadan *et al.* [25] constructed Quadratic Chaotic Map based on Chebyshev map to improve both the chaotic parameter range and maximum Lyapunov exponents (MLEs) to expand the key space of cryptosystem.

However, despite the Chebyshev system can improve the security of image encryption to some extent, there are still some drawbacks that can lead to potential hazard for the cryptosystem. First, the security of Chebyshev-based schemes is generally not high enough because the chaotic dynamic properties degrade rapidly when the chaotic maps are realized with finite precision [15], [16]. Second, initial value of Chebyshev map in a certain range will cause the generated sequence without chaotic property. Moreover, the value distribution of chaotic sequences is not uniform enough, which can reduce the randomness of the sequence and increase the predictability of the secret key.

To overcome the above drawbacks, we construct a new chaotic system and design a color image encryption scheme. The main contributions of our work are as follows.

- A Homogenized Chebyshev-Arnold Map (HCAM) with outstanding cryptography features in dynamics is proposed. It can avoid the drawbacks of the original Chebyshev map when used in image encryption. Based on the HCAM, a novel image encryption algorithm that contains confusion and diffusion stages has been proposed.
- In the confusion stage, we modify the Chaotic Matrix Transform (CMT) to randomize the shifting steps to eliminate the regular pattern of the original CMT, which can obtain higher level of security.
- In the diffusion stage, we design a SHA-based fast pixel substitution method to implement in bit level and achieve outstanding self-adaptiveness and high efficiency.

The whole encryption process involves no conjugated operation between pixels, rows or columns, so our scheme obtain superior robustness against data loss and noise attack. Simulation results and security analysis have been carried out and demonstrate the security of our algorithm in comparison with state-of-the-art algorithms.

## II. THE PROPOSED HOMOGENIZED CHEBYSHEV-ARNOLD MAP

In this section, we first review the original Chebyshev map and analyze its potential problems when used in image encryption. Then, we construct the HCAM by introducing Arnold index to the Chebyshev map. Moreover, the theoretical analysis and contrastive simulations are carried out and demonstrate that our HCAM can avoid the problems of original Chebyshev map. Furthermore, the pseudo-randomness and chaotic properties of the HCAM are also tested to verify its superior capability in image encryption algorithm.

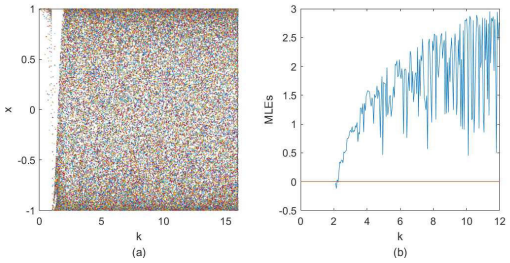



**FIGURE 1.** (a) Bifurcation graph and (b) MLEs with proper initial values of Chebyshev map.

### A. THE ORIGINAL CHEBYSHEV MAP AND ITS PROBLEMS

The original Chebyshev map is an one-dimensional chaotic system with an initial value $x_0$ and a control parameter $k$. It is defined as follows:

$$x_{n+1} = cos(k \times \arccos x_n), \quad x_n \in [-1, 1], \ (n = 0, 1, 2 \ldots) \tag{1}$$

when $k \in (2, +\infty)$, the sequence generated by Chebyshev map is chaotic. The Chebyshev map has been used in image encryption algorithm [22]–[25] due to its outstanding pseudo-randomness and large range of control parameters. The bifurcation diagram and MLEs is presented in Fig. 1.

However, when directly using Chebyshev map to image encryption, the cryptosystem will suffer the following problems:

#### 1) PROBLEM A: INITIAL VALUE IN CERTAIN RANGE LEADS TO NON-CHAOTIC PROPERTY

We divide the range of the initial value $x_0$ of Chebyshev map in (1) as Fig. 2. Through the simulation experiment, when $x_0$ located in Area 1, more times of iterations are needed for chaotic behaviors. If the initial value is in Area 2, no matter how many iteration times, the generated sequence will not obtain chaotic property when $k$ take some particular values. The MLEs is a typical criterion for judging chaotic behaviors of a sequence in dynamical system [26], [27]. Fig. 3(a) shows the MLEs of Chebyshev map when the initial value is 0 (in Area 2), we can see that the results are exactly 0 when $k = 2, 4, 6 \ldots$, which means non-chaotic behaviors [28]. Worse still, when the initial value is near $-1$ or 1, the same phenomenon reproduces. The basic reason for this problem is that once $x_r$ is not located in safety zone in Fig. 2, $x_{r+1}$ will not in safety zone either. With the iteration times increases, such values converge to an extremely narrow range, which

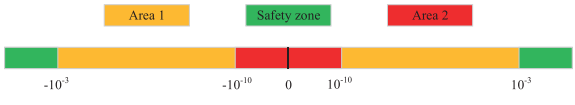



**FIGURE 2.** Safety zone and unsafe areas for initial value around 0 of Chebyshev Map.

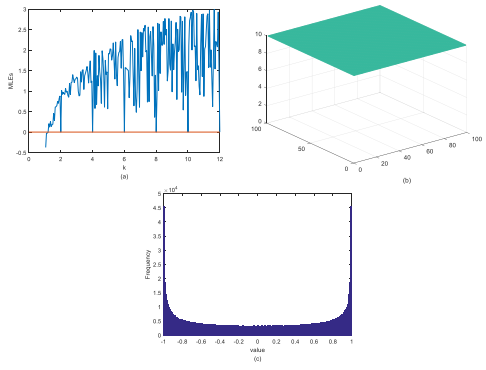


**FIGURE 3.** (a) MLEs (initial value = 0), (b) mutual information, and (c) histogram (length = $10^6$) of Chebyshev map.

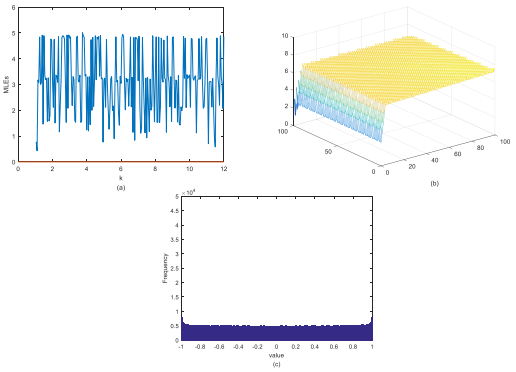


**FIGURE 4.** (a) MLEs (initial value = 0), (b) mutual information and (c) histogram (length = $10^6$) of the proposed HCAM.

leads to non-chaotic behaviors. Therefore, the initial value should be selected carefully for image encryption.

#### 2) PROBLEM B: HIGH MUTUAL INFORMATION

Every new item $x_{i+1}$ of the original Chebyshev map is generated from the previous $x_i$ according to (1). This correlation leads to high mutual information because the uncertainty of $x_{i+1}$ is extremely little if we have known the previous $x_i$. As Fig. 3(b) shows, mutual information of Chebyshev map is much high. Therefore, when directly using the Chebyshev map to image encryption, attackers can acquire the control parameter by repeat substitution operations, which will cause the encryption algorithm invalid totally. To solve this problem, we need to add turbulence to the chaotic system to break the correlation between adjacent items. From above analysis, both of the Problem A and Problem B are caused by the complete correlation relationship between $x_{r+1}(i)$ and $x_r(i)$.

#### 3) PROBLEM C: NON-UNIFORM VALUE DISTRIBUTION

According to Wu *et al.* [29], using non-uniform chaotic sequences to image encryption, ciphertext images can not be encrypted securely. We have tested the values distribution of the chaotic sequences generated by original Chebyshev map, and the result is shown in Fig. 3(c). Obviously, it is not uniform enough, which means the ciphertext images encrypted based on such chaotic sequences may obtain non-uniform histograms and cannot resist the potential statistical attack [29].

### B. THE PROPOSED HCAM

The non-linear maps such as Arnold map, Standard map, and Tent map can construct nonlinear couple, which is very suitable to break the correlation between adjacent Chebyshev items. Since the Arnold map is simple and easy to realize, without loss of generality, we construct an HCAM by homogenizing the coupling of Chebyshev map and Arnold map. It can solve the problems of original Chebyshev map.

#### 1) COUPLING STEP

The proposed HCAM is constructed to improve the weak dynamical behaviors of existing chaotic maps. We combine the original Chebyshev map and Arnold map as follows:

$$x_{n+1}(i)=\cos\{k\mu f(x_n(i-1))+\frac{k}{2}(1-\mu)[f(x_n(p))+f(x_n(q))]\} \tag{2}$$

where $f(x) = \arccos x$, $i, p, q$ are indexes of the sequences, and their relationship is constrained by Arnold map as follows:

$$\begin{bmatrix} p \\ q \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} i \\ i \end{bmatrix} \pmod{L} \tag{3}$$

where $1 \le i, p, q \le L$, $L$ is the length of generated sequence, $x_1(i)$ in (2) are generated by Chebyshev map, $\mu$ controls the coupling degree of Arnold map and it is appropriate in [0.6, 0.96], $n$ refers to iteration times.

Unlike the original Chebyshev map that has complete correlation between adjacent terms, the $x_{r+1}(i)$ of the proposed HCAM is no longer completely related to $x_r(i)$ due to our Coupling Step. Therefore, even if $x_r(i)$ is not located in safety zone, the newly generated values in the following iterations are very likely to hit safety zone, which means the proposed HCAM can solve the Problem A and B.

#### 2) HOMOGENIZATION STEP

To deal with the Problem C, the key task is to homogenize the value distribution in the original range. Here, we use the rule in (4) as a hash function to achieve this purpose. For term $x_n(i)$, update itself by

$$X_n(i) = 2 \times [x_n(i) \times H \ (mod\ 2)] - 1 \tag{4}$$

where $H$ is magnification value, and $X_n(i)$ is the sequence generated by the HCAM.

### C. CHAOTIC ANALYSIS OF THE PROPOSED HCAM

In this part, we first evaluate the performance of the proposed HCAM from the MLEs, mutual information, and histogram distribution. Then, we use Golomb randomness postulates [24] to check the pseudonoise statistical properties. The chaotic behavior of the HCAM is also analyzed from the bifurcation diagram, power and energy perspectives to demonstrate the superior security of the proposed HCAM when used in image encryption algorithm.

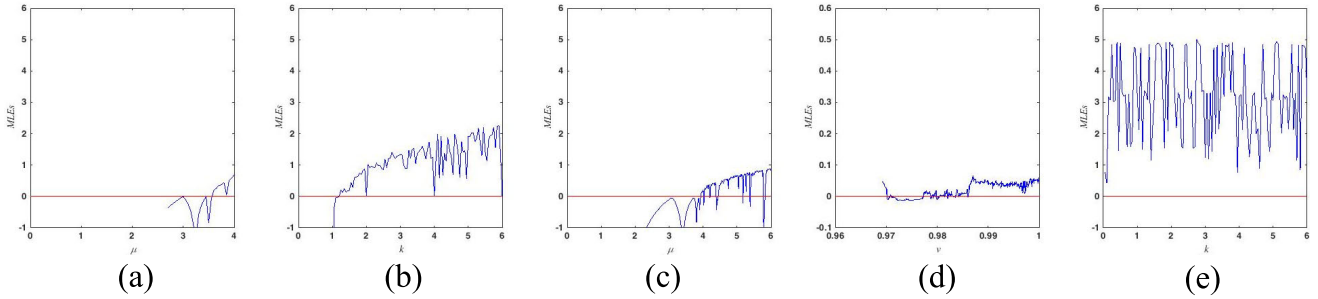



**FIGURE 5.** Maximum Lyapunov exponent of the chaotic map (a) Logistic map, (b) Chebyshev map, (c) Modified Logistic map, (d) F3DHenon, (e) The proposed HCAM.

### 1) SETTLEMENT OF THE THREE PROBLEMS

In order to analyze the dynamic behaviors of the proposed HCAM, we test the MLEs and mutual information. As Fig. 4(a) shows, when the initial value is 0 (in Area 2 of Fig. 2), the MLEs are all above 0, which means the proposed HCAM still has chaotic behaviors and verifies that our HCAM can solve Problem A efficiently. On the other hand, the mutual information of the HCAM is shown in Fig. 4(b). Clearly, it is much lower than the result of original Chebyshev map in Fig. 3(b), which means the determinacy of adjacent items is greatly reduced, so the Problem B is also settled successfully. Furthermore, we also check the distribution of the HCAM, comparing with Fig. 3(c), the histogram of the HCAM in Fig. 4(c) is much more uniform, which demonstrates the chaotic sequence generated by our HCAM is more suitable for image encryption.

In addition, we also compared the MLEs of the proposed HCAM with other chaotic maps and the result is shown in Fig. 5. The plots indicate that compared with the existing chaotic systems, the MLE of our HCAM is larger and more positive, which means it is highly sensitive to initial conditions. Moreover, as can be observed, the range of control parameters of the HCAM can expand to $[0.35, +\infty)$, which means it can significantly extend the key space when used in image encryption.

### 2) PSEUDO-RANDOMNESS PROPERTY OF THE PROPOSED HCAM

To test the pseudo-random character of the proposed HCAM, we follow the Golomb randomness postulates that states an ideal one-dimensional chaotic system should satisfy the following properties [24]:

- Mean value of the sequence is zero.
- The cross-correlation function is zero.
- The shape of autocorrelation function is similar to $\delta$ function.

Our HCAM inherits the excellent pseudonoise statistical properties of the origin Chebyshev map very well. From Fig. 6, we can see that the average values and cross correlation function of the HCAM are both fluctuated around zero, which satisfy the property 1 and 2. And the shape of autocorrelation

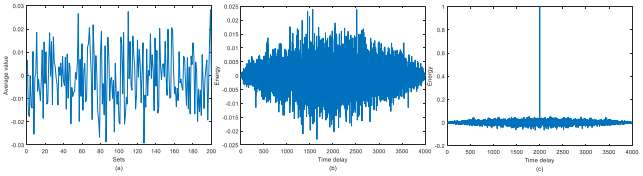


**FIGURE 6.** (a) Average values, (b) cross correlation function of the HCAM (length $= 2 * 10^3$), and (c) autocorrelation function.

function is approximately the same as $\delta$ function, which means that chaotic sequences generated by our HCAM are difficult to predict by statistical attacks. Therefore, image encryption algorithms based on the HCAM will obtain higher security level.

### 3) CHAOTIC PROPERTY OF THE PROPOSED HCAM

The bifurcation diagram is always examined to gain a comprehensive understanding of the dynamics of a chaotic system [30]. Fig. 7 shows the bifurcation structures of the proposed HCAM and some latest developed chaotic maps [30], [31]. As can be observed, the chaotic region of our HCAM is greatly expanded compared with other chaotic maps.

Except the bifurcation diagram and MLEs, chaotic sequences can also be regarded as power signal or energy signal. For power signal, we can observe the shape of power spectral to test the chaotic property [32]. Though some periodic signals show randomness in the time domain, their power spectral often has only one or two peaks, which represents internal systematicness. While the power spectral of a chaotic signal usually has many peaks. As Fig. 8(a) shows, the power spectral of the proposed HCAM does not have obvious minority peaks, which means the HCAM has chaotic property.

For energy signal, principal component analysis (PCA) is often utilized to determine whether certain signal is chaotic [32]. If the principal component spectrum has an obvious decreasing rather than horizontal all the time, the corresponding energy signal is chaotic. Otherwise, the signal is white noise [33]. Fig. 8(b) compares the PCA results of the HCAM and white Gaussian noise. As we can see, when embedding dimension $i \in [1, 2]$, the PCA results of the HCAM decrease rapidly, which means the conspicuous chaotic property.

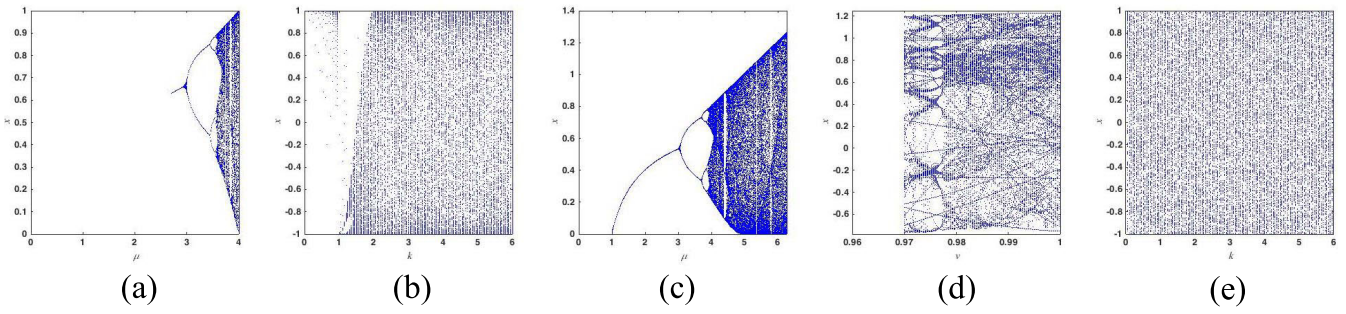



**FIGURE 7.** Bifurcation diagram of the chaotic map (a) Logistic map, (b) Chebyshev map, (c) Modified Logistic map, (d) F3DHenon, (e) The proposed HCAM.

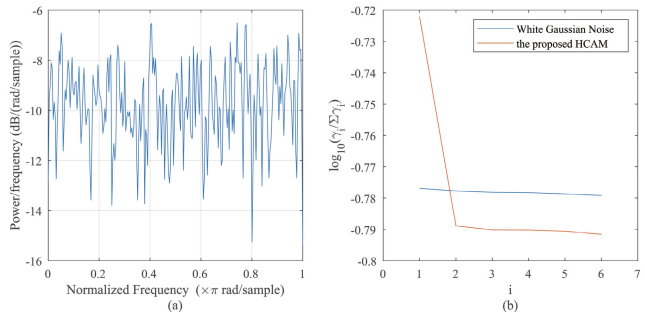



**FIGURE 8.** (a) Power spectral analysis of the proposed HCAM; (b) Comparation of principal component analysis of the proposed HCAM and white Gaussian noise.

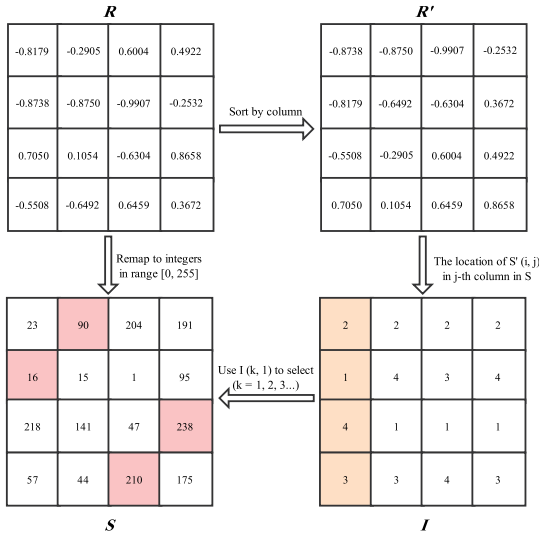



**FIGURE 9.** Flowchart of generating matrix $I$ and $R$.

## III. COLOR IMAGE ENCRYPTION AND DECRYPTION ALGORITHMS

Based on the proposed HCAM, we present a novel color image encryption algorithm that contains two parts: confusion and diffusion. In the confusion stage, we use the RCMT to randomize the shifting steps, which can eliminate the regular pattern of the original CMT [19] and enhance the security level. In the diffusion stage, we use a SHA-512 and SHA-384 based fast pixel substitution scheme to perform the bit-level exclusive-or operation. The details of the proposed algorithm are described below.

### A. CONFUSION STAGE: RANDOM CHAOTIC MAGIC TRANSFORM

In consideration of the high relevance among pixels of an image, we should separate the adjacent pixels to reduce the correlation in confusion stage. The CMT [19] is an efficient algorithm that can shuffle adjacent pixels in short time by simultaneously changing the location of row and column. However, the shifting steps will increase with progressively transform in CMT, which may be exploited by attackers and cause invalid to against chosen plaintext attack [34]. Here, we propose a RCMT to handle this problem.

For an $M \times N$ plaintext image $O$, in the RCMT, we first generate an $M \times N$ chaotic matrix $R$ by the proposed HCAM. And matrix $R'$ is built by sorting $R$ as column. Then, we use matrix $I$ records the location of $R'(i, j)$ in the $j - th$ of matrix $R$. This process is shown in Fig. 9. After getting matrix $R$, $R'$ and $I$, the RCMT can be performed as Algorithm 1. For the $i - th$ iteration, the shifting step is defined as,

$$Step(i) = mod(S(i, I(i, 1)) + Z, N - 1) + 1 \tag{5}$$

where $Z$ is a random integer to ensure us obtain completely different ciphertext images even encrypting the same plaintext image with the same chaotic sequence, which can ulteriorly increase the security level in an extremely simple way. Considering the locations of selected pixels should not remain the same (i.e. $Step(i) = 0$), we add 1 to change the range of $Step(i)$ from $[0, N - 2]$ to $[1, N - 1]$. This process has been marked in matrix $S$ in Fig. 9.

The RCMT can change the row and column location of a pixel simultaneously and does not take extra time complexity. Therefore, it keeps the advantage of low runtime of the CMT. Meanwhile, $Step(i)$ is totally random and unpredictable due to the HCAM and random integer $Z$, which makes our RCMT much more secure than the original CMT.

### B. DIFFUSION STAGE: SHA-BASED FAST PIXEL SUBSTITUTION SCHEME

With the help of the RCMT, the confusion step can break the correlation between adjacent pixels completely and

**Algorithm 1** Random Chaotic Matrix Transform

**Input:** Matrix $R$, $R'$, $I$ and a plaintext image $O$ with the size of $M \times N$

**Output:** Matrix $S$ and a scrambled image $T$ with the size of $M \times N$

Prepare a random integer Z;
Remap $R$ to integers in range [0, 255], and get $S$;
**for** $i = 1$ to $M$ **do**
    $pixels = [O(I(i, 1), 1), O(I(i, 2), 2), \ldots, O(I(i, N), N)]$;
    Link $pixels$ as a circular linked $list$;
    Shift the $list$ $Step(i)$ time(s) in (5);
    Save the updated $list$ to T
**end for**

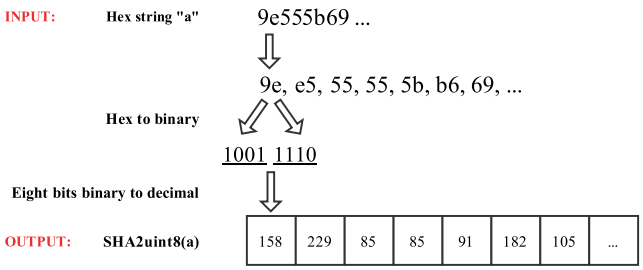



**FIGURE 10.** Flowchart of SHA based pixel substitution scheme.

efficiently. However, the statistical information of plaintext image is not concealed, which makes the ciphertext images can't resist histogram attack. To solve this problem, researchers have proposed various diffusion schemes, which usually use modulo operation to hash the original gray scale towards the whole range to homogenize the histogram of ciphertext image and conceal statistical information [18]. Although modulo-operation-based diffusion schemes are indeed effective, this operation need multiple loops to ensure performance, which is time-consuming. To shorten runtime, we utilize the SHA-512 and SHA-384 of the plaintext image to perform bit-level exclusive-or operation. The flowchart is shown in Fig. 10, and the detailed process is described in Algorithm 2.

Considering the length of SHA-512 and SHA-384 are 128 and 96 and can be split into 127 and 95 pairs of hex characters, the lengths of $rdmSeq512$ and $rdmSeq384$ in Algorithm 2 are fixed as 127 and 95, which makes our algorithm extremely sensitive to the plaintext image. That is, even a bit change on the plaintext image will convert the result completely, which guarantee the resistance of our diffusion scheme against differential attack. Meanwhile, we use the matrix $S$ in Algorithm 1 to save time and further uniformize the distribution of gray scales. As high speed bit-level exclusive-or operations are involved in the entire process, our diffusion process is exceedingly timesaving.

### C. COLOR IMAGE ENCRYPTION ALGORITHM

A color image consists of R, G and B components, which means one color pixel in visual actually depends on three values. Therefore, the color images are more sensitive to noise and data loss because only one of three values in the same location changes during transmission, the corresponding color will not be recovered correctly. In our image encryption algorithm, we utilize RCMT and SHA-based fast pixel substitution scheme to encrypt color images, and the detail process is described in Algorithm 3.

In the confusion step, if we use different $Step(i)$ in each channel, the pixels of the same location will shift to three different locations. When suffering external influence like data loss and salt-pepper noise, it will enlarge the influence three times. To avoid this drawback, in our algorithm, the same

**Algorithm 2** SHA Based Fast Pixel Substitution Scheme

**Input:** Matrix $S$, a plaintext image $O$ and a scrambled image $T$ with the size of $M \times N$

**Output:** A ciphertext image $C$ with the size of $M \times N$

$u = 1$; $v = 1$;
$hexStr512 = SHA\text{-}512(O)$;
$hexStr384 = SHA\text{-}384(O)$;
$rdmSeq512 = SHA2uint8(hexStr512)$;
$rdmSeq384 = SHA2uint8(hexStr384)$;
**for** $i = 1$ to $M$ **do**
    **for** $j = 1$ to $N$ **do**
        $temp1(i, j) = T(i, j) \oplus rdmSeq512(u))$;
        $temp2(i, j) = temp1(i, j) \oplus rdmSeq384(v))$;
        **if** $u == 128$ **then**
            $u = 1$;
        **end if**
        **if** $v == 96$ **then**
            $v = 1$;
        **end if**
    **end for**
**end for**
$C = temp2 \oplus S$;

**Algorithm 3** Color Image Encryption Algorithm

**Input:** A plaintext color image $O$ with the size of $M \times N$

**Output:** A ciphertext color image $C$ with the size of $M \times N$

Here is the same as Line 1-5 in Algorithm 2.
Prepare parameters set $K = \{k, k', \mu, n, H, p, q, X_1(1)\}$
Generate chaotic matrix $R$ using set $K$.
    *// $X_1(1)$ and $k'$ is used to generate $X_1$.*
    */* $p$ and $q$, which are parameters for Arnold map, together with $\mu$, $k$ and $n$, are used in Coupling Step, where $n$ is the iteration times. */*
    *// $H$ is magnification value in Homogenization Step.*
Get RGB components of $O$, marked as $O_R$, $O_G$ and $O_B$
Use Algorithm 1 and the same $R$ to scramb $O_R$, $O_G$ and $O_B$, and get $T_R$, $T_G$ and $T_B$
Use Algorithm 2 and the same $S$ to operate $T_R$, $T_G$ and $T_B$, and get $C_R$, $C_G$ and $C_B$
Combine $C_R$, $C_G$ and $C_B$ to obtain ciphertext image $C$

chaotic matrix $S$ is utilized in R, G and B channels. That is, with the same $Step(i)$ in the RCMT, pixels in the same location of three channels will shift to another same location in ciphertext image, which neither enlarge the external influence, nor lose randomness with the help of the HCAM chaos. Similarly, in the diffusion step, unlike other schemes that use row and column transformation, our SHA based fast pixel substitution scheme mainly involves bit-level exclusive-or operation to substitute a single pixel, which only affects itself and unable enlarge the external influence either. Meanwhile, the SHA of plaintext images can add self-adaptiveness to our algorithm, which contribute to defend differential attack effectively. Therefore, our confusion and diffusion process can ensure the safety and robustness for the color image encryption.

The decryption process is similar to the image encryption, which significantly simplify the implementation of our algorithm. On the one hand, to decrypt the RCMT, we can just make $step(i) = N - step(i)$ and perform Algorithm 1 again. On the other hand, due to the fact that inverse operation of exclusive-or is itself, the diffusion step can be decrypted successfully by applying Algorithm 2 again.

## IV. EXPERIMENTS AND PERFORMANCES

In this section, we perform experiments to demonstrate the capabilities of the proposed image encryption algorithm. The simulations are implemented under MATLAB R2018a on a laptop with Intel(R) Core(TM) i7-6600U CPU, 2.60 GHz. The test images are "Couple", "Woman", "House" and "Lena" with size of $256 \times 256 \times 3$, and the encryption and decryption results are shown in Fig. 11. As can be observed, all of the ciphertext images are similar noise-like although their corresponding plain images have different contents. Attackers can not obtain any original information from the pixel distribution of the ciphertext images visually, which verify the security of the cryptosystem to some extent. Using the correct keys, we can completely recover the plaintext images (Fig.11(c)).

In practical, a good cryptosystem should also robust to potential attacks. Without the correct keys, one can't achieve any information regarding the plaintext images. Only using the correct keys can one correctly recover the original images. Next, some commonly used attacks are tested to indicate the superior security level of our algorithm.

### A. KEY SPACE ANALYSIS

From the cryptographic point of view, the size of the key space should not be smaller than $2^{100}$ to ensure the safety of the cryptosystem [35]. In our algorithm, the encryption process indicates that the keys involved in confusion and diffusion steps are independent. Therefore, we need one chaotic map of the HCAM, random integer $Z$, 512 bits-long SHA512 and 384 bits-long SHA 384. The complete key structure of our scheme is illustrated in Fig. 12. The precisions of 8 parameters of the HCAM is listed in Table 1, and the precisions of Z in Algorithm 1 is $10^{-1}$. Since changing any bit in *SHA-512* and *SHA-384* will lead to unsuccessful decryption, the precision of every bit in *Key.Part3* of Fig.12 is $2^{-1}$. Therefore, the whole key space of the proposed algorithm is $10^{-(-15*3-17-1-1-1-1)} * 2^{(512+384)/4} \approx 10^{133}$. This result is large enough to resist brute-force attack and higher than existing algorithms listed in Table II.

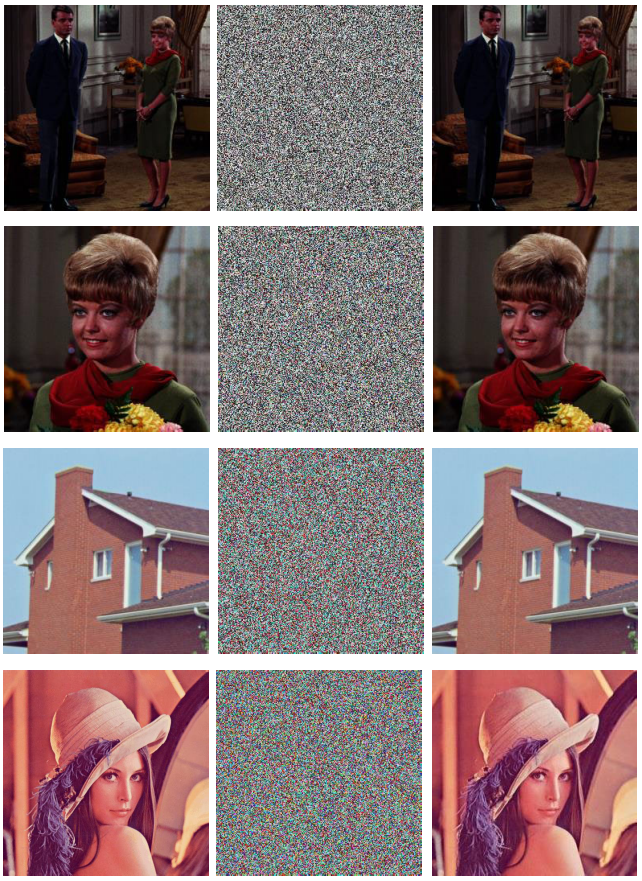



**FIGURE 11.** (a) Left column: Plaintext images; (b) Middle column: Ciphertext images; (c) Right column: Recovered images.

**TABLE 1.** The precisions of 8 parameters of the HCAM.

| Parameter | $k$ | $k'$ | $\mu$ | $H$ |
|---|---|---|---|---|
| Precision | $10^{-15}$ | $10^{-15}$ | $10^{-17}$ | $10^{-1}$ |
| Parameter | $X_1(1)$ | $p$ | $q$ | $n$ |
| Precision | $10^{-15}$ | $10^{-1}$ | $10^{-1}$ | $10^{-1}$ |

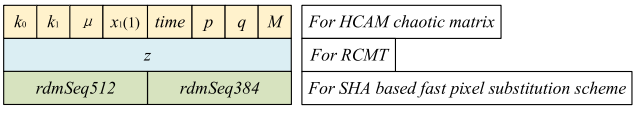



**FIGURE 12.** The key structure of the proposed algorithm.

### B. KEY SENSITIVITY ANALYSIS

For a secure cryptosystem, the ciphertext image should be highly sensitive to the variation of secret keys. To evaluate the key sensitivity of our encryption algorithm, we change one of the secret keys with a tiny difference and other keys remain

**TABLE 2.** Key space comparison.

| Algorithms | Key Space |
|---|---|
| Our proposed algorithm | $10^{133}$ |
| Ref. [7] | $8.39 \times 10^{(22+16L)}$ |
| Ref. [11] | $10^{96}$ |
| Ref. [12] | $2^{480}$ |
| Ref. [16] | $10^{98}$ |
| Ref. [23] | $2^{298}$ |
| Ref. [39] | $5 \times 10^{102}$ |
| Ref. [40] | $5 \times 10^{117}$ |


**FIGURE 13.** Decrypted images with (a) the correct *Key*, (b) incorrect $k$ ($k = k + 10^{-15}$), (c) incorrect $k'$ ($k' = k' + 10^{-15}$), (d) incorrect $\mu$ ($\mu = \mu + 10^{-17}$), (e) incorrect $H$ ($H = H + 1$), (f) incorrect $X_1(1)$ ($X_1(1) = X_1(1) + 10^{-15}$), (g) incorrect $p$ ($p = p + 1$), (h) incorrect $q$ ($q = q + 1$), (i) incorrect $n$ ($n = n + 1$).

the same. Fig. 13 displays the decrypted images with correct key and various wrong keys, as can be observed, there is no valid information can be obtained from Fig. 13 (b)-(i), which demonstrate that even if an extremely tiny change on the correct key will lead to completely unsuccessful decryption. Therefore, our cryptosystem is sensitive to the secret keys and robust against blind decryption.

### C. STATISTICAL ATTACK ANALYSIS

In our algorithm, the diffusion part is indispensable to hide the statistical information of the plaintext images. Next, we will analyze the histogram and correlation of ciphertext images to evaluate the capability of our algorithm against statistical attack.

**TABLE 3.** $\chi^2$ values for plaintext images and ciphertext images in three channels.

| Images | | $\chi^2$ values | | |
|---|---|---|---|---|
| | | R | G | B |
| Couple | Plaintext image | 210349.14 | 305382.04 | 289576.09 |
| | Ciphertext image | 219.54 | 277.33 | 240.70 |
| Girl | Plaintext image | 168940.96 | 146963.05 | 158023.55 |
| | Ciphertext image | 246.81 | 270.87 | 228.38 |
| House | Plaintext image | 258576.88 | 299158.64 | 394038.95 |
| | Ciphertext image | 250.81 | 255.88 | 259.57 |
| Lena | Plaintext image | 59326.50 | 31287.17 | 80935.84 |
| | Ciphertext image | 253.07 | 273.21 | 267.11 |

#### 1) HISTOGRAM ANALYSIS

The histogram can intuitively present the pixel distribution of an image, so it is an useful tool to evaluate the performance of an cryptosystem. An ideal image encryption algorithm should obtain ciphertext images with uniform distributed histograms, which can hide the original statistical information.

Fig. 14 shows the histograms of four plaintext images and their respective ciphertext images in three channels. Compared with the histograms of plaintext images, histograms of ciphertext images distribute much more uniform, which indicate that our algorithm can hide the original pixel distribution effectively.

To quantitatively verify the uniformness of the histograms of ciphertext images, we test the unilateral hypothesis [13]. For an 8-bit gray scale image, its $\chi^2$ values can be calculated by:

$$\chi^2 = \sum_{i=0}^{255} \frac{(o_i - e_i)^2}{e_i} \tag{6}$$

where $o_i$ is occurrence frequency of gray scale level $i$, and $e_i$ is the expected occurrence frequency of the uniform distribution. Given a significant level $\alpha = 0.05$, we have $\chi^2_{0.05}(255) = 293.2478$. Therefore, if the $\chi^2$ value of an image is less than $\chi^2_{0.05}(255)$, the histogram is considered to be uniform. Table 3 shows the $\chi^2$ values of 4 plaintext images and respective ciphertext images in three channels. As can be observed, all $\chi^2$ values of ciphertext images decrease sharply and less than $\chi^2_{0.05}(255)$, which means the histogram of ciphertext images are in uniform distribution.

In addition, based on the quantity analysis in [36], we further evaluate the uniformity of ciphertext images from the variance of histograms and the results are recorded in Table 4. As can be observed, the variance values of ciphertext images are about 500, which indicate that the number of average fluctuation in each gray level is about 20 pixels. However, the variance value is more than $3 \times 10^4$ for plaintext image Lena. And the variance value is about 5000 for image Lena in Zhang's algorithm [36], which is greater than any variance in Table 4. Therefore, our algorithm is efficient and can successfully hide the original statistical information.

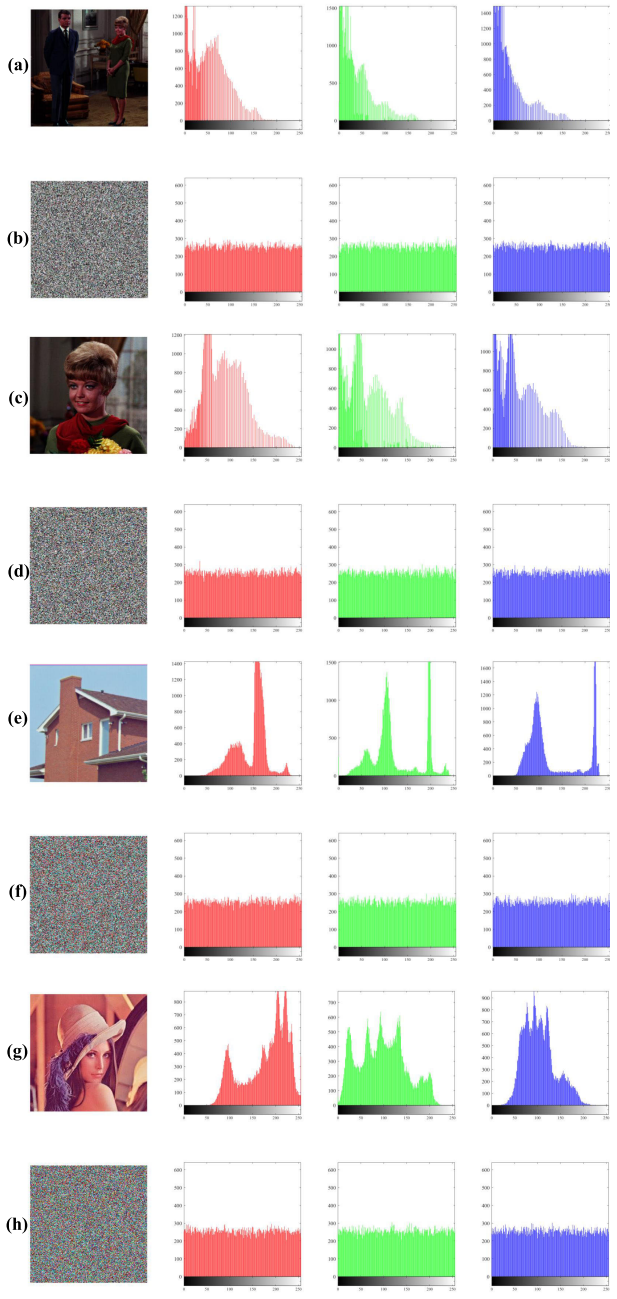



**FIGURE 14.** The histogram of the plaintext images and ciphertext images: (a) Plaintext image Lena; (b) Cipher image Lena; (c) Plaintext image Couple; (d) Cipher image Couple; (e) Plaintext image Woman; (f) Cipher image Woman; (g) Plaintext image House; (h) Cipher image House.

#### 2) CORRELATION ANALYSIS

Correlation analysis is another effective way to evaluate the robustness against statistical attack. The adjacent pixels of plaintext image usually have high correlation coefficients, and a good encryption algorithm should significantly reduce the correlation among adjacent pixels in the ciphertext images. We have calculated the data correlation by (7).

$$Corr = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y} \tag{7}$$

**TABLE 4.** Variances of Histogram of Plaintext and Ciphertext Images.

| Images | | Variance values | | |
|---|---|---|---|---|
| | | R | G | B |
| Couple | Plaintext image | 210920 | 306580 | 290450 |
| | Ciphertext image | 475.44 | 531.94 | 497.05 |
| Girl | Plaintext image | 169350 | 147450 | 158390 |
| | Ciphertext image | 500.73 | 527.74 | 485.08 |
| House | Plaintext image | 259330 | 300330 | 395330 |
| | Ciphertext image | 507.23 | 511.68 | 514.29 |
| Lena | Plaintext image | 59502 | 31262 | 80995 |
| | Ciphertext image | 504.96 | 529.99 | 522.61 |

where $X$ and $Y$ are data sequences, $\mu$ is the mean value and $\sigma$ is the standard deviation. We randomly choose 2000 pairs of adjacent pixels in horizontal, vertical and diagonal direction of the three channels, and use (7) to calculate the correlation coefficients. The results are shown in Fig. 15 and Table 5. Compared with the plaintext images, our algorithm significantly reduce the value of correlation coefficients in ciphertext images, which means the proposed scheme ensures the security successfully.

### D. DIFFERENTIAL ATTACK ANALYSIS

Differential attack is also known as chosen-plaintext attack [34]. An adversary may make a tiny change on the plaintext image, and then observes the differences between two ciphertext images to deduce the keys of cryptosystem. In this way, a meaningful relationship between two ciphertext images and the plaintext images can be utilized to attack the cryptosystem. A good encryption algorithm should have the ability to resist the differential attack. This usually be evaluated by NPCR (number of pixels change rate) and UACI (unified average changing intensity):

$$\begin{cases} D(i,j) = \begin{cases} 1, & c_1(i,j) \neq c_2(i,j) \\ 0, & otherwise \end{cases} \\ NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \end{cases} \tag{8}$$

$$UACI = \frac{1}{M \times N}[\sum_{ij} \frac{c_1(i,j) - c_2(i,j)}{255}] \times 100\% \tag{9}$$

where $c_1$ and $c_2$ are two ciphertext images whose corresponding plain images have only one pixel difference.

As Wu suggests [29], we test the NPCR and UACI with critical value to show the validity of defending differential attack. Table 6 records the NPCR results of three channels, we use the most rigorous $N^*_{0.05}$ to examine (Pass if $NPCR > 99.5693\%$ for $256 \times 256$ images). Results of various ciphtertext images obtained by our algorithm pass the $N^*_{0.05}$ test. Compared with existing schemes, for the same images (“Lena” and “baboon”), our results are the highest, which means the strongest ability against differential attack. For UACI tests, we evaluate the results with 5 different images in three channels by examining the most rigorous $N^{*-}_{0.05}$ and $N^{*+}_{0.05}$ (Pass if $33.2824\% < UACI < 34.6447\%$ for

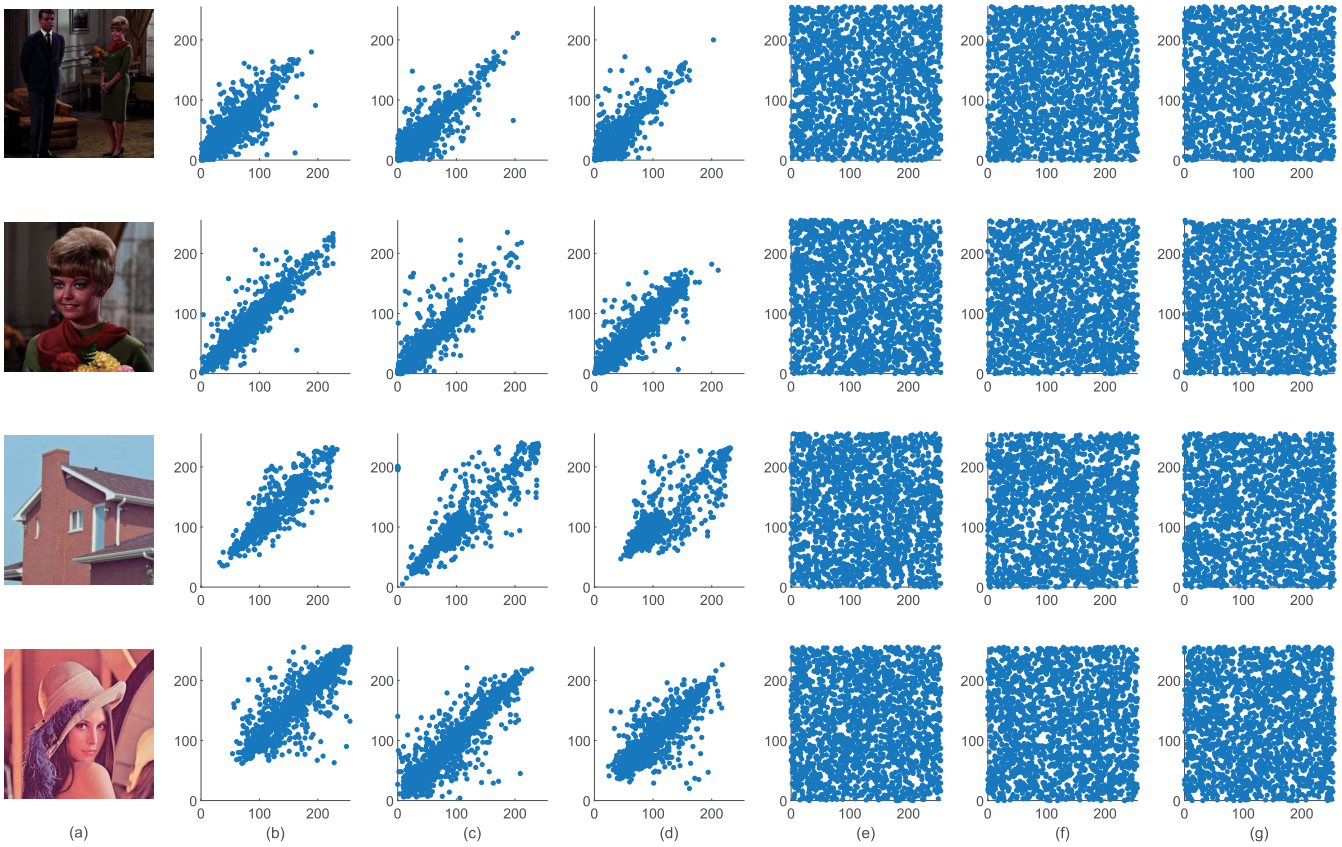



**FIGURE 15.** (a) Plaintext images; (b)-(d) Correlation of plaintext images: (b) R; (c) G; (d) B; (e)-(g) Correlation of ciphertext images: (e) R; (f) G; (g) B.

**TABLE 5.** Comparison of NPCR test results for different color images in three channels.

| Images | Directions | Plaintext images | | | Ciphertext images | | |
|---|---|---|---|---|---|---|---|
| | | R | G | B | R | G | B |
| Couple | Horizontal | 0.9509 | 0.9191 | 0.9277 | 0.0331 | 0.0007 | -0.0021 |
| | Vertical | 0.9564 | 0.9366 | 0.9531 | 0.0335 | -0.0063 | 0.0022 |
| | Diagonal | 0.9292 | 0.8952 | 0.8867 | -0.0176 | -0.0038 | -0.0101 |
| Girl | Horizontal | 0.9759 | 0.9733 | 0.9585 | 0.0347 | -0.0097 | 0.0133 |
| | Vertical | 0.9608 | 0.9715 | 0.9419 | 0.0071 | 0.0087 | 0.0045 |
| | Diagonal | 0.9412 | 0.9450 | 0.9411 | 0.0093 | -0.0187 | -0.0024 |
| House | Horizontal | 0.9655 | 0.9794 | 0.9825 | 0.0298 | -0.0004 | -0.0110 |
| | Vertical | 0.9346 | 0.9557 | 0.9762 | 0.0026 | -0.0039 | 0.0292 |
| | Diagonal | 0.9103 | 0.9416 | 0.9566 | -0.0397 | 0.0141 | 0.0112 |
| Lena | Horizontal | 0.9522 | 0.9463 | 0.8983 | -0.0786 | -0.0079 | 0.0230 |
| | Vertical | 0.9717 | 0.9727 | 0.9434 | 0.0443 | 0.0236 | -0.0047 |
| | Diagonal | 0.9385 | 0.9189 | 0.8389 | 0.0498 | -0.0032 | 0.03362 |

$256 \times 256$ images). From Table 7, all UACI values pass the $N^{*-}_{0.05}$ and $N^{*+}_{0.05}$ test, which further illustrates the high security level of our algorithm.

### E. INFORMATION ENTROPY

The information entropy is a valid criterion to judge the randomness of gray scale values distribution and complexity of a system [37]. To calculate the entropy $H(s)$ of an image, we use (10)

$$H(s) = -\sum_{i=0}^{2^n-1} P(s_i) log_2 P(s_i) \tag{10}$$

where $P(s_i)$ represents the probability of the symbol $s_i$. For a perfectly random signal consisting of $2^n$ symbols, $H(s)$ is equal to 8. The higher of the entropy value, the more random of ciphertext images. Table 8 lists the results of four

**TABLE 6.** Comparison of NPCR test results for different color images in three channels.

| Algorithms | Images | NPCR | | | Results |
|---|---|---|---|---|---|
| | | R | G | B | Pass / Fail |
| Our Algorithm | Couple | 99.59% | 99.59% | 99.59% | Pass |
| | Girl | 99.60% | 99.60% | 99.60% | Pass |
| | House | 99.66% | 99.66% | 99.66% | Pass |
| | Baboon | 99.66% | 99.66% | 99.66% | Pass |
| | Lena | 99.69% | 99.69% | 99.69% | Pass |
| Ref. [7] | Lena | 99.59% (Gray image) | | | Pass |
| Ref. [11] | Lena | 99.65% (Gray image) | | | Pass |
| Ref. [12] | Lena | 99.60% | 99.60% | 99.61% | Pass |
| Ref. [16] | Lena | 99.99% | 99.99% | 99.99% | Pass |
| Ref. [23] | Lena | 99.60% | 99.61% | 99.60% | Pass |
| Ref. [38] | Lena | 99.36% (Average) | | | Failed |
| Ref. [39] | Lena | 99.71% (Average) | | | Pass |
| Ref. [40] | Lena | 100% (Average) | | | Pass |

**TABLE 7.** Comparison of UACI test results for different color images in three channels.

| Algorithms | Images | UACI | | | Results |
|---|---|---|---|---|---|
| | | R | G | B | Pass / Fail |
| Our Algorithm | Couple | 33.47% | 33.52% | 33.51% | Pass |
| | Girl | 33.51% | 33.48% | 33.45% | Pass |
| | House | 33.54% | 33.60% | 33.47% | Pass |
| | Baboon | 33.49% | 33.52% | 33.52% | Pass |
| | Lena | 33.35% | 33.45% | 33.42% | Pass |
| Ref. [7] | Lena | 33.25% (Gray image) | | | Failed |
| Ref. [11] | Lena | 33.48% (Gray image) | | | Pass |
| Ref. [12] | Lena | 33.50% | 33.49% | 33.44% | Pass |
| Ref. [16] | Lena | 33.34% | 32.95% | 33.30% | Failed |
| Ref. [23] | Lena | 33.47% | 33.54% | 33.54% | Pass |
| Ref. [38] | Lena | 32.72% (Binary image) | | | Failed |
| Ref. [39] | Lena | 33.45% | | | Pass |
| Ref. [40] | Lena | 33.44% | | | Pass |

**TABLE 8.** Comparison for information entropy of plaintext images and ciphertext images in three channels.

| Algorithms | Images | | Information Entropy | | |
|---|---|---|---|---|---|
| | | | R | G | B |
| Our Algorithm | Couple | Plaintext | 7.2136 | 6.9325 | 7.1238 |
| | | Ciphertext | 7.9995 | 7.9995 | 7.9995 |
| | Girl | Plaintext | 7.3490 | 7.1876 | 6.9857 |
| | | Ciphertext | 7.9994 | 7.9995 | 7.9994 |
| | House | Plaintext | 7.1837 | 7.0926 | 6.8057 |
| | | Ciphertext | 7.9995 | 7.9995 | 7.9995 |
| | Lena | Plaintext | 7.2531 | 7.5940 | 6.9684 |
| | | Ciphertext | 7.9993 | 7.9994 | 7.9993 |
| Ref. [7] | Lena | Ciphertext | 7.9971 (Gray image) | | |
| Ref. [11] | Lena | Ciphertext | 7.9970 (Gray image) | | |
| Ref. [12] | Lena | Ciphertext | 7.9994 | 7.9993 | 7.9993 |
| Ref. [16] | Lena | Ciphertext | - | | |
| Ref. [23] | Lena | Ciphertext | 7.9994 | 7.9994 | 7.9994 |
| Ref. [38] | Lena | Ciphertext | 7.9801 (Binary image) | | |
| Ref. [39] | Lena | Ciphertext | 7.9973 | | |
| Ref. [40] | Lena | Ciphertext | 7.9991 | | |

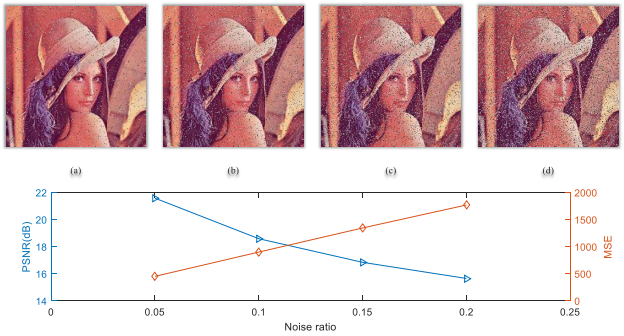



**FIGURE 16.** Decrypted images with noise attack (a) 5% salt-pepper noise; (b) 10% salt-pepper noise; (c) 15% salt-pepper noise; (d) 20% salt-pepper noise.

plaintext images and respective ciphertext images. Compared with plaintext images, the information entropy of ciphertext images all increase and approach to 8, which means the gray scale distribution of three channels of ciphertext images are all uniform. Therefore, the output of our algorithm tends to be ideally ciphertext images with extraordinary randomness [29] and unlikely divulge any valid information.

### *F. ROBUSTNESS AGAINST DATA LOSS AND NOISE ATTACK*

When transmitting on insecure channels, the ciphertext images may be clipped by attackers or polluted by noises. Because our algorithm involves no conjugated operation between pixels, rows or columns, the obtained ciphertext images have superior robustness against data loss and noise. To test the tolerance of our algorithm against noise attacks, we add salt & pepper noise to the ciphertext images and decrypt them with correct keys. The results are shown in Fig. 16, as can be observed, the meaningful information of plain images can be recognized, which demonstrates that our method is robust to noise attack.

To verify the robustness of our method against data loss, we occlude some portion of ciphertext images and decrypt them with correct keys. Fig. 17 shows the data-loss images and the corresponding decrypted images. It can be seen that even occlude 75% information in ciphertext images, the main content of plaintext image can also be retrieved successfully with a certain image quality degradation, which demonstrate the strong capability of our method in dealing with the distortions caused by data-loss.

### *G. ENCRYPTION/DECRYPTION SPEED*

The proposed algorithm can achieve a relatively high encryption speed because of two factors: First, we use RCMT to separate adjacent pixels in only one-time transform; Second, the whole diffusion process mainly involves bit-level exclusive-or operation, which is believed to be a fairly fast operation. Since our algorithm possesses identical encryption and decryption process, it consumes the same time on encrypting/decrypting an image with same size. We have

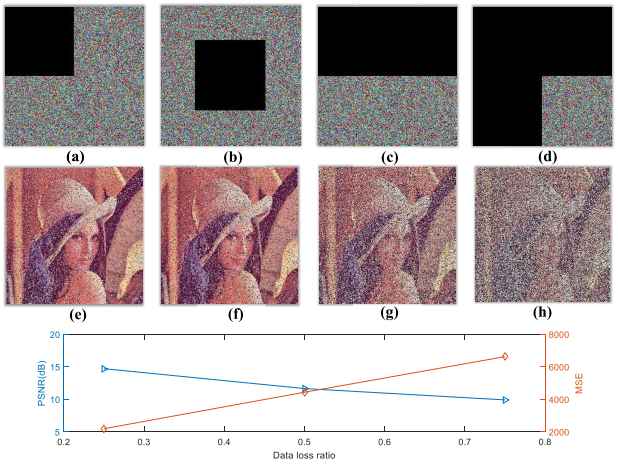



**FIGURE 17.** The ciphertext images with data loss attack (a) 25% data loss; (b) 25% data loss; (c) 50% data loss; (d) 75% data loss. The decrypted images with correct keys (e) decryption of (a); (f) decryption of (a); (b) decryption of (c); (h) decryption of (d).

**TABLE 9.** Time cost for different schemes to encrypt different size of images. (Time(s)).

| Algorithms | Image | 256×256 | 512×512 | 1024×1024 |
|---|---|---|---|---|
| **Our Algorithm** | **Encryption** | **0.1789** | **1.0351** | **7.1335** |
| | **Decryption** | **0.1673** | **1.1187** | **7.0095** |
| **Ref. [7]** | **Gray image** | - | 0.1750 | - |
| **Ref. [12]** | **Color** | 0.0025 | 0.01 | 0.042 |
| **Ref. [23]** | **Color** | - | 0.29 | - |
| **Ref. [38]** | **Binary image** | 7.55 | - | - |
| **Ref. [39]** | **Color** | 1.85 | 3.76 | 26.34 |
| **Ref. [40]** | **Color** | 0.58 | 2.28 | 9.16 |

implemented the program using MATLAB language and the results are listed in Table 9. Although the speed of our method is not faster than some real-time encryption algorithm [12], [23], it is also efficient compared with some similar algorithm [38]–[40].

## V. CONCLUSION

In this paper, we construct a chaotic system called HCAM with complex chaotic behavior. Based on it, a new color image encryption algorithm is proposed. In the confusion stage, we apply the RCMT to randomize the shifting steps and obtain higher level of security. Thereafter, a fast SHA-based pixel substitution method is operated in bit level with outstanding self-adaptiveness and high efficiency. Simulation results verify that our algorithm is at high security level. In the future work, we attempt to implement the proposed HCAM chaotic system in a parallel version to further improve its efficiency. In addition, we will extend the related applications of HCAM and RCMT for image security.

## REFERENCES

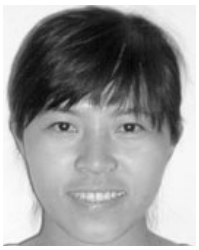
[1] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2005.
[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[3] W. Feng, Y. He, H. Li, and C. L. Li, "Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map," *IEEE Access*, vol. 7, pp. 12584–12597, 2019.
[4] J. Yu, Y. Li, X. Xie, N. Zhou, and Z. Zhou, "Image encryption algorithm by using the logistic map and discrete fractional angular transform," *Optica Applicata*, vol. 47, no. 1, pp. 141–155, 2017.
[5] S. Kumar and R. K. Sharma, "Securing color images using two-square cipher associated with Arnold map," *Multimed Tools Appl.*, vol. 76, pp. 8757–8779, Mar. 2017.
[6] A. M. Elshamy, F. E. A. El-Samie, O. S. Faragallah, E. M. Elshamy, H. S. El-Sayed, S. F. El-Zoghdy, A. N. Z. Rashed, A. El-Naser A. Mohamed, and A. Q. Alhamad, "Optical image cryptosystem using double random phase encoding and Arnold's cat map," *Opt Quant Electron*, vol. 48, no. 3, p. 212, 2016.
[7] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.
[8] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010.
[9] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011.
[10] 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.
[11] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
[12] X. Wang, L. Feng, and H. Y. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
[13] Z. Yong, "The unified image encryption algorithm based on chaos and cubic S-box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.
[14] S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei, "A new plaintext-related image encryption scheme based on chaotic sequence," *IEEE Access*, vol. 7, pp. 30344–30360, 2019.
[15] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.
[16] X. Kang, A. Ming, and R. Tao, "Reality-preserving multiple parameter discrete fractional angular transform and its application to color image encryption," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 6, pp. 1595–1607, Jun. 2019.
[17] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.*, vol. 26, pp. 10–20, Jan. 2015.
[18] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.
[19] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.
[20] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.
[21] T. Geisel and V. Fairen, "Statistical properties of chaos in Chebyshev maps," *Phys. Lett. A*, vol. 105, no. 6, pp. 263–266, 1984.
[22] C. Fu, J.-J. Chen, H. Zou, W.-H. Meng, Y.-F. Zhan, and Y.-W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Opt. Express*, vol. 20, no. 3, pp. 2363–2378, 2012.
[23] B. Stoyanov and K. Kordov, "Image encryption using chebyshev map and rotation equation," *Entropy*, vol. 17, no. 4, pp. 2117–2139, 2015.
[24] L. Wang, Q. Ye, Y. Xiao, Y. Zou, and B. Zhang, "An image encryption scheme based on cross chaotic map," in *Proc. Congr. Image Signal Process. (CISP)*, vol. 3, May 2008, pp. 22–26.
[25] N. Ramadan, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El-Samie, "Chaos-based image encryption using an improved quadratic chaotic map," *Amer. J. Signal Process.*, vol. 6, no. 1, pp. 1–13, 2016.
[26] D. C. Karnopp, D. L. Margolis, and R. C. Rosenberg, *System Dynamics: A Unified Approach*, vol. 514, 2nd ed. New York, NY, USA: Wiley, 1990.
[27] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.
[28] H. Kantz, "A robust method to estimate the maximal Lyapunov exponent of a time series," *Phys. Lett. A*, vol. 185, no. 1, pp. 77–87, Jan. 1994.

[29] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommu.*, vol. 1, pp. 31–38, Apr. 2011.
[30] L. Jouini, A. Ouannas, A.-A. Khennaoui, X. Wang, G. Grassi, and V.-T. Pham, "The fractional form of a new three-dimensional generalized Hénon map," *Adv. Difference Equ.*, vol. 2019, p. 122, Dec. 2019.
[31] S. Hanis and R. Amutha, "A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure," *Nonlinear Dyn.*, vol. 95, no. 1, pp. 421–432, Jan. 2019.
[32] D. S. Broomhead and G. P. King, "Extracting qualitative dynamics from experimental data," *Phys. D, Nonlinear Phenomena*, vol. 20, nos. 2–3, pp. 217–236, 1986.
[33] M. Suk and S. Hong, "An edge extraction technique for noisy images," *Comput. Vis., Graph., Image Process.*, vol. 25, no. 1, pp. 24–45, 1984.
[34] 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.
[35] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken, NJ, USA: Wiley, 1996.
[36] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[37] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 511–529, 2015.
[38] J. Ahmad and S. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1839–1850, Dec. 2015.
[39] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
[40] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

**XUEJING KANG** received the B.S. and M.S. degrees from the Tianjin University of Technology, in 2008 and 2012, respectively, and the Ph.D. degree from the Beijing Institute of Technology. She is currently a Lecturer with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. Her current research interests include fractional Fourier transform, image processing, and computer vision.

**XUANSHU LUO** is currently pursuing the bachelor's degree with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include image processing and human–computer interaction.

**XUESONG ZHANG** (M'13) received the Ph.D. degree in pattern recognition and intelligent systems from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2009. He is currently a Senior Researcher with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing. His current research interests include computer vision, computational imaging, and machine learning.



**JING JIANG** received the B.S. degree in automation from the China University of Mining Technology (CUMT), Xuzhou, China, in 2002, and the M.S. and Ph.D. degrees in communication and information systems from CUMT, Beijing (CUMTB), China, in 2008 and 2012, respectively. She is currently an Associate Professor with the Department of Communication Engineering, Beijing Union University, Beijing. Her research interests include image processing and computer vision.