On the Use of Memristive Hyperchaotic System to Design Color Image Encryption Scheme

XIAOYUAN WANG, (Member, IEEE), MENG GAO, XIAOTAO MIN, ZHUOSHENG LIN, AND HERBERT HO-CHING IU, (Senior Member, IEEE)

1School of Electronics and Information, Hangzhou Dianzi University, Hangzhou 310018, China
2Faculty of Intelligent Manufacturing, Wuyi University, Jiangmen 529020, China
3School of Electrical, Electronic and Computer Engineering, The University of Western Australia, Perth, WA 6009, Australia

Corresponding authors: Xiaoyuan Wang (youyuan-0213@163.com) and Zhuosheng Lin (zhuoshenglin@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61871429 and Grant 61901304, and in part by the Natural Science Foundation of Zhejiang Province under Grant LY18F010012.

ABSTRACT

In this article a novel encryption scheme based on memristive hyperchaotic system was proposed. Firstly, combined with SHA-512 hash function and plain image, key sequences can be generated by iterating the memristive hyperchaotic system. Then, permutation operation and diffusion operation are performed for each row and column of the plain image. Finally, a serious of simulation experiments are conducted to evaluate the proposed encryption scheme, showing that the proposed scheme has well performance. Further, NIST SP800-22 test results show that the randomness of the hyperchaotic pseudorandom sequence used by the algorithm is better than the general linear congruence pseudorandom sequence.

INDEX TERMS

Memristive, hyperchaos, image encryption, NIST SP800-22.

I. INTRODUCTION

The existence of Memristor is predicted by Chua in 1971 [1]. It was not until 2008, the nano-membrane memristive device was made by HP and immediately intrigued wide spread concern in both academia and industry [2]. After years of development, the memristive system has been applied in analog circuits [3], chaotic system [4], memory [5], neural networks [6], image encryption [7], et al.

As we can see now, there are social platforms such as Facebook, Twitter and WeChat let people connect with friends and family to share tidbits of their life. This makes large amounts of images are transmitted and stored over internet, including some with personal privacy. Thus, the demand for image encryption has become urgent. Since there are natural similarities between chaos and cryptograph, such as sensitive to initial conditions and parameters, pseudorandomness and ergodicity, it leads to a serious search to design chaos-based image encryption methods [8]–[11]. These proposed encryption methods are range from the used of chaotic system only to combined chaotic system with other interrelated fields. For example, a hyperchaotic image encryption algorithm was proposed in [9], which scrambles the image by Logistic mapping sequences, and then diffuses the image by high-dimensional chaotic sequences. However, the security flaw is that one byte plaintext data can affect only one byte ciphertext data. In [10], an image encryption algorithm based on the memristive hyperchaotic system, cellular automata, and DNA sequence operations are proposed. In which, cellular automata DNA sequence operations are used to enhance the security of encryption algorithm. Besides, in order to improve the security, multi rounds of permutation-diffusion mechanism are used [12], [13]. And in each round, the diffusion operation can be performed only if all the permutation operations are completed. Actually, by using these two mechanisms, computational complexity will increase, but for a practical encryption algorithm should make balance between security and speed.

Based on the above analyses, a novel memristive hyperchaotic system-based color image encryption scheme is introduced. In the proposed scheme, SHA-512 and plain image are used to give the initial values of memristive hyperchaotic system, making that the generated key sequences are sensitive to the plain image. The permutation operation and diffusion operation are performed for each row and column of the plain image, after each row or column permutation operation is completed, the corresponding diffusion operation can be performed immediately.

The rest of this article is organized as follows. Section II introduces the memristive hyperchaotic system and its
discretization. The image encryption scheme is described in Section III. Simulation results and security analyses are presented in Section IV. Section V discusses the performance of pseudorandom sequences. The last Section concludes the paper.

II. MEMRISTIVE HYPERCHAOTIC SYSTEM AND ITS DISCRETIZATION

According to [14], the memristive system was derived as

\[
\begin{align*}
\frac{dx}{dt} &= a(y - x) + b(x + \beta w^2)y \\
\frac{dy}{dt} &= cx - xz \\
\frac{dz}{dt} &= x^2 - dz \\
\frac{dw}{dt} &= y,
\end{align*}
\]

(1)

where \(x, y, z\) and \(w\) are internal state variables, \(a, b, c, d, \alpha\) and \(\beta\) are parameters. By selecting \(a = 24, b = 4, c = 19, d = 9, \alpha = 1\) and \(\beta = 0.02\), the system behaves hyperchaos. The Lyapunov exponents are calculated as \(\lambda_1 = 0.3399, \lambda_2 = 0.2144, \lambda_3 = -0.0045, \lambda_4 = -33.5498\), and the Lyapunov dimension is \(D_L = 3.0164\). Figure 1 shows the chaotic attractor.

To implement the above system on the digital software platform, the system need to be discretized firstly. By using Euler method, the memristive system (1) can be derived as

\[
\begin{align*}
\frac{x(n + 1) - x(n)}{\Delta t} &= a(y(n) - x(n)) + b(x + \beta w^2(n)y(n)) \\
\frac{y(n + 1) - y(n)}{\Delta t} &= cx(n) - x(n)z(n) \\
\frac{z(n + 1) - z(n)}{\Delta t} &= x(n)x(n) - dz(n) \\
\frac{w(n + 1) - w(n)}{\Delta t} &= y(n).
\end{align*}
\]

(2)

Then, one can obtain the discrete-time memristive system as

\[
\begin{align*}
x(n + 1) &= x(n) + a(y(n) - x(n)) + b(x + \beta w^2(n)y(n)) \Delta t \\
y(n + 1) &= y(n) + [cx(n) - x(n)z(n)] \Delta t \\
z(n + 1) &= z(n) + [x(n)x(n) - dz(n)] \Delta t \\
w(n + 1) &= w(n) + y(n) \Delta t,
\end{align*}
\]

(3)

where the sampling time is set as \(\Delta t = 0.001\), and the initial values are set as \(x(0) = 0.01, y(0) = 0.01, z(0) = 0.01, w(0) = 0.01\). Keeping the parameters \(a, b, c, d, \alpha\) and \(\beta\) unchanged, the corresponding phase diagrams are shown in Figure 2. Compared with Figure 1, it can be seen that the discrete-time memristive system (3) maintains the dynamic characteristics and the complex topological structure in phase space.

III. ENCRYPTION SCHEME

In this article, the encryption scheme is aimed at color RGB images. In order to improve the security performance, the scheme repeatedly performs permutation and diffusion operations during encryption and decryption.

A. GENERATION OF INITIAL VALUES FROM PLAIN IMAGE

In order to against chosen-plaintext attack, Hash function is used to change the initial values of Eq. (3). Firstly, SHA-512 is selected to obtain the hash value of the plain image. As shown in Figure 3, the hash value \(H\), which contains 512 bits, is divided into 64 blocks \(h_1, h_2, \ldots, h_{64}\) and each block contains 8 bits.

Then, one can obtain the disturbance values \(k_1, k_2, k_3, k_4\) as

\[
\begin{align*}
k_1 &= h_1 \oplus h_5 \oplus \cdots \oplus h_{61} \\
k_2 &= h_2 \oplus h_6 \oplus \cdots \oplus h_{62} \\
k_3 &= h_3 \oplus h_7 \oplus \cdots \oplus h_{63} \\
k_4 &= h_4 \oplus h_8 \oplus \cdots \oplus h_{64},
\end{align*}
\]

(4)
As the chaotic sequences generated by Eq.(3) are floating-point data, the sequences need to be processed before using for encryption. One can obtain the key sequences $S_1 = \{s_1^1, s_1^2, \ldots, s_1^{M\times N\times 3}\}$, $S_2 = \{s_2^1, s_2^2, \ldots, s_2^{M\times N\times 3}\}$ as

$$\begin{align*}
S_1 & = \text{mod}(\text{round}(X \times 10^{15}), 256) \\
S_2 & = \text{mod}(\text{round}(Y \times 10^{15}), 256),
\end{align*}$$

where $\text{mod}(\cdot, 256)$ is a modular function, and $\text{round}(\cdot)$ is a round down operation.

**C. IMAGE ENCRYPTION ALGORITHM**

The plain image is divided into three channels R, G, and B, and each channel is a $M \times N$ matrix. The key sequences $S_1, S_2$ can be divided into three components $S_1^R, S_1^G, S_1^B$ and $S_2^R, S_2^G, S_2^B$. As shown in Figure 4, each of them is used for encrypting the three channels R, G, and B respectively. Since the encryption algorithm for three channels R, G, B are similar, here the encryption algorithm for channel R is taken as an example.

**Step 1: Dividing the key sequences**

The key sequences $S_1^R$ is divided into $M$ groups in front-to-back order, and the length of each group is $N$.

**Step 2: Designing the permutation operation**

Each row of channel R is taking out and performed a cyclic shift. Here, a cyclic right shift is carried out, and the shift number is by the first data of each key sequence. Then, a new matrix $R'$ can be obtained.

**Step 3: Designing the diffusion operation**

The first row of matrix $R'$ is exclusives or with first group of $S_1^R$ byte by byte, and the first row of the diffused matrix is formed as $R^1$. Then the second row of R will exclusive or with $R^1$ first, then exclusive or with the corresponding group of $S_1^R$. And the following other rows of matrix will are executed in the same way, that is exclusive or with the previous diffused...
row first, and then exclusive or with the corresponding group of $S_1^R$. Finally, a new matrix $R^{row}$ can be obtained.

It is worth to point out that in the proposed algorithm after each row permutation operation is completed, the corresponding row diffusion operation can be performed immediately. This feature is different from the diffusion operation performed only if all the permutation operations are completed in traditional schemes. In addition, due to the particularity of Step 3, each row of ciphertext is not only related to the corresponding row of plaintext, but also related to the previous rows of plaintext.

After performing the above row operation on image matrix, the column operation is followed, which is similar with row operation. The difference is that the input plain image and the key sequences are change to $R^{row}$, $S_1^R$ respectively, and $S_2^R$ is divided into $N$ groups with the length of $M$.

The complete process of encryption diagram is shown in Figure 5. After performing row operation and column operation, the ciphertext data $R^{(e)}$, $G^{(e)}$, $B^{(e)}$ can be obtained. The encryption algorithm for channel G and B are similar. By recombining cipher text data $R^{(e)}$, $G^{(e)}$, $B^{(e)}$, the cipher image can be obtained.

IV. PERFORMANCE ANALYSIS AND COMPARISON

As shown in Figure 6, the standard color image Lena with size $512 \times 512$ is used as plain image to demonstrate the proposed encryption scheme.

A. EXPERIMENT RESULT

The encrypted image and the decrypted is shown in Figure 7. From Figure 7(a), we can see that the encrypted is completely noisy without any obvious textural features. Form Figure 6 and Figure 7(b), the decrypted image is consistent with the original one, indicating that the decrypted image can recover the features of the original image. Thus, the proposed encryption scheme achieves a good effect.

Even though the original image is pure white or pure black, the proposed encryption scheme can also achieve a good performance. Figure 8 shows the corresponding encrypted and decrypted images of pure white image and pure black image, respectively.
B. HISTOGRAM ANALYSIS

The histograms of the plain image and encrypted image are shown in Figure 9. From Figures 9(a), 9(c) and 9(e), we can see the distribution of histograms of original image is extremely uneven and have spikes. However, after encrypted, the histograms have a completely uniform distribution, which indicated that the statistical properties of the plain image are disturbed by the proposed encryption scheme.

C. CORRELATION ANALYSIS

Generally, there is strong correlation between the adjacent pixels of an image. Analysts often use this feature to crack the encryption scheme. So, one of the important aspects of a secure encryption scheme is to reduce the correction between the adjacent pixels.

The correlation between the plain image and its corresponding encrypted image can be calculated via

$$\rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}}$$  \hspace{1cm} (8)

where $x, y$ represent the adjacent pixels of images, and $N$ is the number of randomly selected pixels, which is equal to 10,000 in here. Noted that the correlation coefficients of uncorrelated sequences should be zero theoretically. As shown in Table 1, the correlation of the original image is strong. After encrypted, the correlation coefficients are closed to 0.

On the other hand, by randomly taking pixels from the image, the pixel values distributions of adjacent pixels in horizontal, vertical and diagonal direction of plain image and its corresponding encrypted images are shown in Figure 10. We can see from Figures 10(a), 10(c) and 10(e) that the correlation between adjacent pixels of the plain image is high, which is densely arranged on a linear function like.

The expressions of cov$(x, y)$ and $D(\cdot)$ are as follow:

\[
\begin{align*}
\text{cov}(x, y) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \\
D(x) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2 \\
E(x) &= \frac{1}{N} \sum_{i=1}^{N} x_i
\end{align*}
\]  \hspace{1cm} (9)
D. DIFFERENTIAL ANALYSIS

When performing a differential attack, the attacker usually makes a slight adjustment to the plaintext, and then performs the attack by comparing the difference between the ciphertext of original plaintext and the ciphertext of slightly adjusted plaintext. For image encryption differential analysis, the number of changing pixel rate (UACI) and the unified averaged changed intensity (NPCR) are two quantities used for evaluation, which can be calculated by

\[
\begin{align*}
UACI &= \frac{1}{M \times N} \sum_{i,j=0}^{M,N} \left| C_1(i,j) - C_2(i,j) \right| \\
NPCR &= \frac{M \times N}{M \times N} \times 100% 
\end{align*}
\]

(10)

where \(M, N\) are the number of rows and columns of an image, \(C_1(i,j)\) and \(C_2(i,j)\) are the pixel values of two images in coordinate point \((i,j)\) respectively. And \(D(i,j)\) is defined as

\[
D(i,j) = \begin{cases} 
0, & C_1(i,j) = C_2(i,j) \\
1, & C_1(i,j) \neq C_2(i,j)
\end{cases}
\]

In order to avoid accidental test results, 100 coordinate points of the original image are randomly selected for this test. By changing only one pixel once in the original image, 100 plain images with slight changes can be obtained. The encrypted image of original image and the encrypted image of one slight change plain image are formed as a pair of test sample. So that 100 pairs of test samples can be obtained. The NPCR and UACI results are shown in Figure 11.

As shown in Figure 11, the NPCR values of the proposed encryption scheme are approximately stable at 99.6%, and the UACI values are approximately stable at 33.4%. For two random image data, the ideal values of NPCR and UACI are 99.6094% and 33.4635%, respectively. As shown in Figure 11, the values of NPCR and UACI are very close to these ideal values, which show that the encryption algorithm has excellent performance to against differential attack.

E. KEY SENSITIVITY AND KEY SPACE ANALYSIS

The secure encryption scheme is not only sensitive to changes in the plaintext, but also to slight modifications in keys. To this end, a key with tiny change is used to decrypt the cipher image Figure 7(a). The decrypted key is set as follow

\[
\begin{align*}
x(0) &= 0.01 + \frac{k_1}{255} \\
y(0) &= 0.01 + \frac{k_2}{255} + 10^{-15} \\
z(0) &= 0.01 + \frac{k_3}{255} \\
w(0) &= 0.01 + \frac{k_4}{255}
\end{align*}
\]

(11)

And the pixel values of adjacent pixels of the encrypted image are uniformly distributed in the plane as shown in Figures 10(b), 10(d), 10(f). Combined with the results shown in Table 1 and Figure 10, the proposed encryption scheme has good performance to against statistical attacks.
As shown in Figure 12, the corresponding decrypted image is quite different from the plain image. Based on some similar experiments, the sensitivity for initial values are shown in Table 2. The results indicated that the proposed encryption scheme is extremely sensitive to keys.

In order to resist brute force attack, a secure should have a key space of at least \(2^{100} \approx 1.3 \times 10^{30}\). When initial values \(x(0), y(0), z(0)\) and \(w(0)\) are at the range of \([-10, 10]\) and parameter \(d\) is at the range of \([6, 10]\), the memristive system (3) can generate hyperchaos. Assume that precision of floating-point numbers is \(10^{-10}\), so the key space of initial values is \(2^{100}\). After adding parameter \(d\), the total key space is \(6.4 \times 10^{55}\), which is much larger than \(2^{100}\). According to the IEEE-754 floating-point arithmetic standard, the precision of floating-point numbers is \(10^{-15}\). Therefore, the key space will be larger in practical applications.

### F. INFORMATION ENTROPY

The image entropy reflects the average amount of information in the image, which can be used to measure the randomness of the image. The formula is as follows

\[
H(s) = - \sum_{i=0}^{2^n-1} p(s_i) \log_2 p(s_i),
\]

where \(n\) is the bit-length of \(s_i, p(s_i)\) is the probability of \(s_i\). For grayscale images, which consist of \(2^8\) pixel values, the ideal value of information entropy is 8.

The information entropy of gray image obtained by different entropy scheme is compared in Table 3. Table 4 compared the RGB channel information entropy of color image. We can see from Tables 3, 4 that the information entropy of the proposed encryption scheme is closed to the ideal value and the performance of the proposed scheme is similar to that of others. This indicates that the encrypted image has good randomness.

### G. SPEED ANALYSIS

Besides security, speed is an important aspect for an encryption scheme. For a good encryption scheme, it should make balance between security and speed. In the proposed encryption scheme, the iteration number of the memristive hyperchaotic system is \(M \times N \times 3 + P\). The permutation operation and the diffusion operation for row and column are single-round operations without any iteration. Therefore, for the scale of question is the size of image, the order of magnitude for time complexity is \(O(n)\). The comparison of computation time between the proposed encryption scheme and some exciting schemes is show in Table 5. From this table, we can see that the computation time of the proposed one is shorter when the image size is \(256 \times 256\), which indicated that the time complexity is lower. In addition, the computation time for the image size of \(512 \times 512\) is 1.187s. It can be seen that increasing the image size will reduce the encryption speed, because a larger image has more data, which increases the calculation time of the algorithm. In summary, the proposed encryption scheme is good for practical application.

### V. NIST SP800-22 TEST

The security of a stream cipher is closely related to the randomness of the generated sequence. Thus, how to design a pseudorandom sequence with good statistical properties is important. At present, linear congruence generator is one of the most used pseudorandom number generators, which can
be described as

\[ X_{n+1} = (aX_n + c) \mod m, \]

where \( m \) is the modulus, \( a \) is the multiplier, and \( c \) is the increment. The pseudorandom sequence obtained by linear congruence and the memristive hyperchaotic system (3) are both floating-point numbers. After performing amplitude expansion, rounding, and modulo 2, the generated pseudorandom sequences are quantized to the range of \((0, 1)\).

NIST SP800-22 Test Suite is the widely used standard in industry, which included 15 tests. The official documentation of NIST test states that the P-VALUE of the test result greater than 0.01 means the test passes. Moreover, the larger the value of P-VALUE is, the better the result is. By performing NIST SP800-22 test to the above pseudorandom sequences, the test results are shown in Table 6. We can see from Table 6 that both pseudorandom sequences pass all 15 tests. As the P-VALUE of 10 tests of the hyperchaotic pseudorandom sequence is larger than the linear congruence pseudorandom sequence, which indicated that the hyperchaotic pseudorandom sequence has better randomness.

### VI. CONCLUSION

This article studies the discretization of memristive hyperchaotic system. On this basis, an encryption scheme combining permutation and diffusion is proposed. In which, after each row or column permutation operation is completed, the corresponding diffusion operation can be performed immediately. Based on a serious of performance analysis, it was found that the proposed scheme has good statistical properties and is sensitive to keys. By compared with some other encryption schemes, the results show that the proposed scheme is more secure and higher speed. Furthermore, the NIST SP800-22 test results show that the randomness of the hyperchaotic pseudorandom sequence is better than the general linear congruence pseudorandom sequence. Therefore, the proposed encryption scheme has the value of practical application.

### TABLE 6. NIST test results of linear congruence and hyperchaotic pseudorandom sequences.

| statistical results            | linear congruence pseudorandom sequence | hyperchaotic pseudorandom sequence |
|-------------------------------|----------------------------------------|-----------------------------------|
|                               | P-VALUE   | PROPORTION | P-VALUE   | PROPORTION |
| Frequency                     | 0.186566  | 1.00       | 0.190936  | 1.00       |
| Block Frequency               | 0.964295  | 1.00       | 0.970573  | 1.00       |
| Cumulative Sums               | 0.484646  | 1.00       | 0.563482  | 1.00       |
| Run                           | 0.148094  | 1.00       | 0.162066  | 1.00       |
| Longest Run                   | 0.350485  | 0.99       | 0.437274  | 0.96       |
| Rank                          | 0.585209  | 0.99       | 0.654467  | 0.99       |
| FPT                           | 0.888137  | 0.99       | 0.105618  | 0.98       |
| Non-Overlapping Template      | 0.949602  | 1.00       | 0.911413  | 1.00       |
| Overlapping Template          | 0.074177  | 1.00       | 0.242986  | 1.00       |
| Universal                     | 0.875539  | 0.98       | 0.895163  | 0.99       |
| Approximate Entropy           | 0.862344  | 1.00       | 0.848716  | 1.00       |
| Random Excursions Variant     | 0.947557  | 0.98       | 0.976724  | 0.98       |
| Serial                        | 0.934318  | 1.00       | 0.865697  | 1.00       |
| Linear Complexity             | 0.551026  | 0.99       | 0.122325  | 1.00       |
|                               | 0.195163  | 0.99       | 0.232760  | 0.99       |

### REFERENCES

[1] L. Chua, “Memristor–The missing circuit element,” IEEE Trans. Circuit Theory, vol. IT-18, no. 5, pp. 507–519, Sep. 1971.

[2] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, “The missing memristor found,” Nature, vol. 453, no. 7191, pp. 80–83, May 2008.

[3] Z. I. Mannan, S. P. Adhikari, H. Kim, and L. Chua, “Global dynamics of Chu corsage memristor circuit family: Fixed-point loci, Hopf bifurcation, and coexisting dynamic attractors,” Nonlinear Dyn., vol. 99, no. 4, pp. 3169–3196, Mar. 2020.

[4] B. C. Bao, H. Bao, N. Wang, M. Chen, and Q. Xu, “Hidden extreme multistability in memristive hyperchaotic system,” Chaos, Solitons Fractals, vol. 94, pp. 102–111, Jan. 2017.

[5] M. Escudero, I. Vourkas, A. Rubio, and F. Moll, “Memristive logic in crossbar memory arrays: Variability-aware design for higher reliability,” IEEE Trans. Nanotechnol., vol. 18, pp. 635–646, 2019.

[6] N. Li and W. X. Zheng, “Passivity analysis for quaternion-valued memristor-based neural networks with time-varying delay,” IEEE Trans. Neural Netw. Learn. Syst., vol. 31, no. 2, pp. 639–650, Feb. 2020.

[7] G. Peng and F. Min, “Multistability analysis, circuit implementations and application in image encryption of a novel memristive chaotic circuit,” Nonlinear Dyn., vol. 90, no. 3, pp. 1607–1625, Nov. 2017.

[8] J. Ahmad and S. O. Hwang, “A secure image encryption scheme based on chaotic maps and affine transformation,” Multimedia Tools Appl., vol. 75, no. 21, pp. 13951–13976, Nov. 2016.

[9] A. Anees, A. M. Siddiqui, and F. Ahmed, “Chaotic substitution for highly autocorrelated data in encryption algorithms,” Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 9, pp. 3106–3118, Sep. 2014.

[10] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, “An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations,” Signal Process., Image Commun., vol. 52, pp. 6–19, Mar. 2017.

[11] A. Kadir, A. Hamdulla, and W.-Q. Guo, “Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN,” Optik, vol. 125, no. 5, pp. 1671–1675, Mar. 2014.

[12] A. Belazi, A. A. Abd El-Latif, and S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,” Signal Process., vol. 128, pp. 155–170, Nov. 2016.

[13] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, “An efficient image encryption scheme using lookup table-based confusion and diffusion,” Nonlinear Dyn., vol. 81, no. 3, pp. 1151–1166, Aug. 2015.

[14] X. Wang, X. Lin, P. Zhou, and D. Yu, “Hyperchaotic circuit based on memristor feedback with multistability and symmetries,” Complexity, vol. 2020, pp. 1–10, Feb. 2020.

[15] X. Zhang, Z. Zhou, and Y. Niu, “An image encryption method based on the feistel network and dynamic dna encoding,” IEEE Photon. J., vol. 10, no. 4, Jul. 2018, Art. no. 901014.

[16] R. Premkumar and S. Anand, “Secured and compound 3-D chaos image encryption using hybrid mutation and crossover operator,” Multimedia Tools Appl., vol. 78, no. 8, pp. 9577–9593, Apr. 2019.
L. Guo, J. Chen, and J. Li, “Chaos-based color image encryption and compression scheme using DNA complementary rule and chinese remainder theorem,” in Proc. 13th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMITIP), Dec. 2016, pp. 208–212.

J.-F. Zhao, S.-Y. Wang, L.-T. Zhang, and X.-Y. Wang, “Image encryption algorithm based on a novel improper fractional-order attractor and a wavelet function map,” J. Electr. Comput. Eng., vol. 2017, pp. 1–10, Mar. 2017.

R. Rhouma, S. Meherzi, and S. Belghith, “OCML-based colour image encryption,” Chaos, Solitons Fractals, vol. 40, no. 1, pp. 309–318, Apr. 2009.

XIAOYUAN WANG (Member, IEEE) received the B.S. degree in agricultural electrification and automation from Heilongjiang Bayi Agricultural University, Daqing, China, in 2003, the M.S. degree in physical electronics from the Harbin Institute of Technology, Shenzhen, China, in 2008, and the Ph.D. degree in electronic engineering from the Harbin Institute of Technology, Harbin, China, in 2013. From 2010 to 2011, she was a Visiting Student with The University of Western Australia, Australia, where she was also a Visiting Scholar, in 2017. She is currently an Associate Professor with the School of Electronics and Information, Hangzhou Dianzi University. Her research interests include nonlinear dynamics, memristive systems, multiple-valued logic technologies, and signal processing. She has published over 40 articles in these areas.

MENG GAO received the bachelor’s degree in business administration from the School of Business, Jiaxing University, China, in 2019. He is currently pursuing the M.S. degree in integrated circuit engineering with Hangzhou Dianzi University. His current research interests include memristive chaotic circuits and encryption algorithms based on chaotic systems.

XIAOTAO MIN received the B.Eng. degree in communication engineering from the School of Physics and Electronic Information, Gannan Normal University, China, in 2017, and the M.Eng. degree in electronic science and technology from Hangzhou Dianzi University, in 2020. His current research interests include chaotic and hyperchaotic circuit and memristor-based logic circuit design approaches.

ZHUSHENG LIN received the B.Sc. degree in electronic information science and technology and the Ph.D. degree in control science and engineering from the Guangdong University of Technology, Guangzhou, China, in 2013 and 2018, respectively. He is currently a Lecturer with Wuyi University, Jiangmen, China. His research interests include the chaos theory and secure communication, and multimedia privacy protection.

HERBERT HO-CHING IU (Senior Member, IEEE) received the B.Eng. degree (Hons.) in electrical and electronic engineering from The University of Hong Kong, Hong Kong, in 1997, and the Ph.D. degree from The Hong Kong Polytechnic University, Hong Kong, in 2000. In 2002, he joined the School of Electrical, Electronic and Computer Engineering, The University of Western Australia, as a Lecturer, where he is currently a Professor. His research interests include power electronics, renewable energy, nonlinear dynamics, current sensing techniques, and memristive systems. He has authored over 100 articles in these areas. He serves as an Editorial Board Member of the IEEE Journal on Emerging and Selected Topics in Circuits and Systems and the International Journal of Circuit Theory and Applications. He was a recipient of the two IET Premium Awards, in 2012 and 2014, the Vice-Chancellor’s Mid-Career Research Award, in 2014, and the IEEE PES Chapter Outstanding Engineer, in 2015. He also serves as an Associate Editor for the IEEE Transactions on Circuits and Systems—II: Express Brief, the IEEE Transactions on Power Electronics, IEEE Access, IEEE Circuits and Systems Magazine, IET Power Electronics, and the International Journal of Bifurcation and Chaos. He is also a Co-Editor of Control of Chaos in Nonlinear Circuits and Systems (Singapore: World Scientific, 2009) and a Co-Author of Development of Memristor Based Circuits (World Scientific, 2013).

* * *