IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 30, 2019, accepted August 17, 2019, date of publication August 27, 2019, date of current version September 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937767

A Novel Plaintext-Related Image Encryption Algorithm Based on Stochastic Signal Insertion and Block Swapping

SHULIANG SUN, YONGNING GUO, AND RUIKUN WU
Engineering Research Center for ICH Digitalization and Multi-Source Information Fusion, Fuqing Branch of Fujian Normal University, Fuqing 350300, China
Key Laboratory of Nondestructive Testing, Fuqing Branch of Fujian Normal University, Fuqing 350300, China

Corresponding authors: Shuliang Sun (tjussl_07@126.com), Yongning Guo (guoyn@163.com), and Ruikun Wu (dxxfq@fjnu.edu.cn)

This work was supported in part by the Natural Science Foundation of Fujian Province of China under Grant 2018J01788, in part by the Applied Subject Training Program for Electronics and Information Engineering in Fujian Province University, Outstanding Youth Scientific Research Training Program in Fujian Province University, and in part by the Program for New Century Excellent Talents in Fujian Province University.

ABSTRACT Image encryption is an important method for protecting private data during communication. This paper proposes a novel hyperchaotic image encryption algorithm based on stochastic signal insertion and block permutation. First, the 5D hyperchaotic system is applied to generate pseudorandom number sequences. The SHA-256 hash function and secret keys are used to produce the initial values of the cryptosystem. The hash values can effectively enhance the sensitivity to plain image. To enlarge the key space and change orbit of cryptosystem, some stochastic signals are inserted during iteration. The plain image is equally divided into two parts. An X-coordinate, a Y-coordinate and a control table are established with produced pseudonumber sequences. The pixel is swapped with another pixel in the current block or another block depending on the control table. Cyclic shift is performed during the diffusion process. Performance and security analyses are executed to verify the effect of the proposed scheme. It is clear that the proposed scheme has a large key space and is highly sensitive to plain image and secret keys. Moreover, the cryptosystem has low computation complexity and can resist correlation analysis, entropy analysis, statistical attack, differential attack, noise and data loss attacks.

INDEX TERMS Stochastic signal insertion, block permutation, 5D hyperchaotic system, SHA-256 hash function.

I. INTRODUCTION

With the development of Internet and communication techniques, it is increasingly convenient to transmit information over the Internet. Protecting private and confidential data from malicious attacks has become an important issue when transmitting over insecure communication channels. Some techniques have been proposed recently to protect private data, such as steganography [1]–[3], watermarking [4]–[7], and encryption [8]–[12]. Image encryption is an important method in information security, and many schemes have been proposed. These algorithms are based on DNA coding [13]–[15], compressive sensing [16]–[19], QR codes [20]–[22], chaotic systems [23]–[32] and others [33]–[38]. Image encryption schemes based on chaotic system are currently very popular. However, some of these algorithms have been proven insecure [39]–[44]. Low-dimensional chaotic systems are easy to perform, but they have a small key space and few system parameters. The performance of low-dimensional chaotic systems is weak [27]. The hyperchaotic map has at least two positive Lyapunov exponents. The hyperchaotic systems have more variables and parameters, a more complex structure, better ergodicity, wider chaotic intervals and better dynamic performance [23], [27], [45]. Yuan *et al.* [23] proposed a parallel image cryptosystem using a 5D hyperchaotic system. A plain image was divided into levels, and pixels within the same level were processed parallelly. Each pixel was determined by two encrypted pixels which were nearest to its neighbor level. Cao *et al.* [26] presented a new 2D logistic ICMIC cascade map. The scheme was designed to simultaneously perform bit-level permutation and diffusion. Circular shifting was applied in bit-level permutation, and exclusive or (xor) was carried during bit-level diffusion. Xu *et al.* [29]

The associate editor coordinating the review of this article and approving it for publication was mahmoud Barhamgi.

introduced a chaotic image encryption method which was based on block image scrambling and dynamic diffusion. First, the plain image was divided into two equal blocks. Then, an X-coordinate, a Y-coordinate and swapping tables were established. Finally, a dynamic index method was used for a diffusion process. In [35], Hua et al. presented a novel medical image encryption algorithm using high-speed permutation and pixel adaptive diffusion. First, random data was inserted into the surroundings of the image. Then, two rounds of scrambling and diffusion were performed to randomly shuffle neighboring pixels and diffuse these random data over the entire image. The principle of diffusion and confusion were fulfilled in [43]. Random values were added to a plain image to enhance the security of the cryptosystem. The authors in [45] proposed a color image encryption method using hyperchaotic Lorenz systems. Impulse signals were randomly injected into the Lorenz system during iterations. Indeterminate multiple impulse signals can enlarge the key space of cryptosystem. Belazi *et al.* [49] proposed a medical image encryption scheme based on chaos and DNA encoding. SHA-256 hash function and initial secret keys were used to generate the initial values of the chaotic systems.

This paper adopts a 5D hyperchaotic system to produce chaotic sequences for image encryption. To increase the security of the cryptosystem, some stochastic signals are randomly inserted into one of the variables during the iterative process. Stochastic signal insertion can change the chaotic orbit and increase the dynamic behavior of cryptosystem. The key space of the cryptosystem will be enlarged. The SHA-256 hash function is employed to obtain the initial values of the cryptosystem. Therefore, the proposed scheme is closely connected to the original image. A swapping control table is constructed during image scrambling, which moves the pixel far from its relevant scrambling pixel. Cyclic shift is executed to enhance the diffusion effect. Experimental results reveal that the proposed scheme is very fast and highly secure compared with some existing methods.

The rest of this paper is organized as follows. In Section II, the 5D hyperchaotic system is explained, and stochastic signals are inserted. The proposed system is described in Section III. Experimental results are given in Section IV. System evaluation is reported in Section V, and the conclusion is provided in Section VI.

II. 5D HYPERCHAOTIC SYSTEM AND STOCHASTIC SIGNAL INSERTION

A. 5D HYPERCHAOTIC SYSTEM

The 5D hyperchaotic system (system (1)) is described in Eq. (1) [23].

$$\begin{cases} \dot{x}_1 = 30(x_2 - x_1) + x_2x_3x_4 \\ \dot{x}_2 = 10(x_1 + x_2) + x_5 - x_1x_3x_4 \\ \dot{x}_3 = -15.7x_2 - 5x_3 - 2.5x_4 + x_1x_2x_4 \\ \dot{x}_4 = -4.45x_4 + x_1x_2x_3 \\ \dot{x}_5 = -38.5(x_1 + x_2) \end{cases} \tag{1}$$

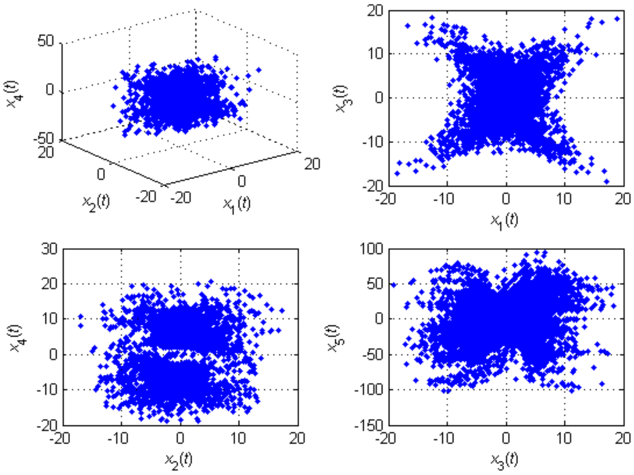


FIGURE 1. The hyperchaotic attractors of system (1).

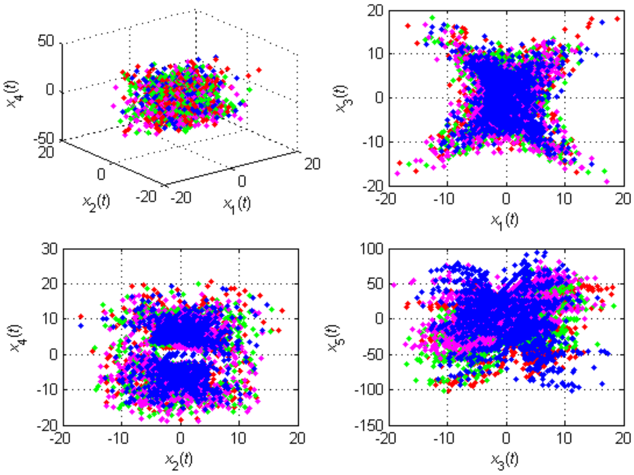


FIGURE 2. The hyperchaotic attractors of system (1) with different colors in four intervals.

The Lyapunov exponents (LEs) of system (1) are 5.12, 0.9, 0, -10.41 and -25.08. There are two positive LEs, and it is a hyperchaotic system. The hyperchaotic attractors of system (1) are shown in Fig. 1.

B. STOCHASTIC SIGNAL INSERTION

To increase the security of the cryptosystem, stochastic signals are randomly inserted into one of the variables when pseudorandom sequences are generated [45]. Stochastic signal insertion can change the chaotic orbit and increase the dynamic behavior of the cryptosystem. Assume the size of plain image I is $M \times N$, and the total number of iterations of system (1) is MN. Then, insert stochastic signals δ_{x_1}, δ_{x_2} and δ_{x_3} into x_1, x_2 and x_3 when the number of iterations $n = \lfloor MN/4 \rfloor$, $\lfloor MN/2 \rfloor$ and $\lfloor 3MN/4 \rfloor$. Here $\delta_{x_i} = [0.5 \min(x_i), 0.5 \max(x_i)]$, and $i = 1, 2, 3$. Four intervals are $[1, \lfloor MN/4 \rfloor - 1]$, $[\lfloor MN/4 \rfloor, \lfloor MN/2 \rfloor - 1]$, $[\lfloor MN/2 \rfloor, \lfloor 3MN/4 \rfloor - 1]$ and $[\lfloor 3MN/4 \rfloor, MN]$. The hyperchaotic attractors of system (1) in the four intervals are shown in different colors of red, green, magenta and blue, as shown in Fig. 2.

III. THE PROPOSED SYSTEM

A. SYSTEM INITIATION

The SHA-256 hash function is used to produce a 256-bit hash value according to a plain image [11]. Even if there is only a slight difference between two images, the hash values will be totally different from each other [16]. The generated hash value is used to produce the initial values of the cryptosystem. The 256-bit hash value K is divided into 8-bit binary blocks. Each binary block is turned into a decimal digit. There are 32 decimal digits, and they are assigned as $k_1, k_2, \ldots, k_{32}$.

The initial values of system (1) can be computed as follows:

$$b = \sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N} I_{x,y}^2 + a} \tag{2}$$

$$h_w = \mathrm{mod}(k_{3w-2} \oplus k_{3w-1} + k_{3w}, 256) \quad (w = 1, 2, \ldots, 10) \tag{3}$$

$$x_1^0 = \mathrm{mod}\left(\frac{h_1}{256} + \frac{b}{2 \times 255} + t_1, 1\right) \tag{4}$$

$$x_j^0 = \mathrm{mod}\left(\frac{h_j}{256} + x_{j-1}^0 + t_j, 1\right) \quad (j = 2, 3, 4, 5) \tag{5}$$

where control parameter a is used to resist a black image attack and $a \in [1, 255]$; t_i is part of the secret key, $i = 1, \ldots, 5$; $\mathrm{mod}(c, d)$ obtains the remainder of c divided by d; and $e \oplus f$ represents the XOR operation between e and f.

B. IMAGE CONFUSION

The plain image is equally divided into two parts, I_1 and I_2, in the horizontal direction. The size of each subimage is $M' \times N'$; here $M' = M/2, N' = N$.

Step 1. Choose randomly a, t_i $(i = 1, \ldots, 5)$ and δ_{x_j} $(j = 1, 2, 3)$ as the initial secret keys.

Step 2. Iterate system (1) 800 times to remove the transient effect. Continue to iterate $M'N'$ times. If the number of iterations is equal to $\lfloor M'N'/4 \rfloor$, $\lfloor M'N'/2 \rfloor$ and $\lfloor 3M'N'/4 \rfloor$, then insert δ_{x_1}, δ_{x_2} and δ_{x_3} into x_1, x_2 and x_3. Continue iterating the chaotic system to generate sequences x_1, x_2, x_3, x_4 and x_5.

Step 3. Generate new sequences s_1 and s_2.

$$\begin{aligned} s_1 &= \mathrm{mod}((abs(x_1 + x_2) - floor(abs(x_1 + x_2))) \\ &\quad \times 10^{15}), M') + 1 \end{aligned} \tag{6}$$

$$\begin{aligned} s_2 &= \mathrm{mod}((abs(x_3 + x_4) - floor(abs(x_3 + x_4))) \\ &\quad \times 10^{15}), N') + 1 \end{aligned} \tag{7}$$

$$V_1 = \mathrm{reshape}(s_1, M', N') \tag{8}$$

$$V_2 = \mathrm{reshape}(s_2, M', N') \tag{9}$$

where $abs(x)$ represents the absolute value of x, $floor(y)$ denotes the nearest integer to y towards minus infinity, and $s_1 \in [1, M']$, $s_2 \in [1, N']$.

Step 4. Form TX, TY and ST as Eqs. (10-12) [29].

$$TX = \begin{cases} \mathrm{mod}(V_1(i,j) + M'/4, M') + 1, & abs(V_1(i,j) - i) < M'/4 \\ V_1(i,j), & otherwise \end{cases} \tag{10}$$

$$TY = \begin{cases} \mathrm{mod}(V_2(i,j) + N'/4, N') + 1, & abs(V_2(i,j) - i) < N'/4 \\ V_2(i,j), & otherwise \end{cases} \tag{11}$$

$$ST = \begin{cases} 1, & abs(V_1(i,j) - i) < M'/4 \\ 1, & abs(V_2(i,j) - i) < N'/4 \\ 0, & otherwise \end{cases} \tag{12}$$

Step 5. Swap pixels in each subimage.

if $ST(i,j) = 0$, exchange $I_1(i,j)$ with $I_1(TX(i,j), TY(i,j))$ and exchange $I_2(i,j)$ with $I_2(TX(i,j), TY(i,j))$;

if $ST(i,j) = 1$, exchange $I_1(i,j)$ with $I_2(TX(i,j), TY(i,j))$ and exchange $I_2(i,j)$ with $I_1(TX(i,j), TY(i,j))$.

Step 6. Connect I_1 and I_2 to form scrambled image SI with size $M \times N$.

The plain image peppers is scrambled using a confusion scheme, and the result is shown in Fig. 3. Figure 3 (c) and (d) are scrambled block images. The histograms of the plain image, scrambled image and scrambled block images are shown in Fig. 4.

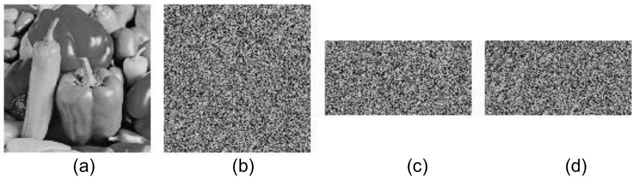


FIGURE 3. Image scrambling performance: (a) Plain image, (b) Scrambled image, (c-d) Scrambled block images.

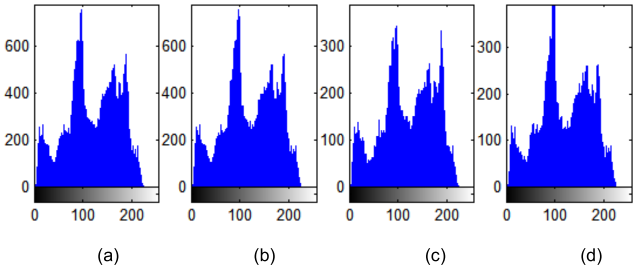


FIGURE 4. Image histogram: (a) Plain image, (b) Scrambled image, (c-d) Scrambled subimages.

It can be seen from Fig. 4 that the histograms of the two scrambled subimages I_1 and I_2 are almost the same as each other, and they are similar to that of scrambled image *SI*. It can also be concluded that there are almost twice as many pixels in scrambled image *SI* as those in each subimage.

C. IMAGE DIFFUSION

Diffusion is indispensable in image encryption scheme. It can extend a tiny change in the original image to the whole encryption image [11]. The steps of the diffusion process are depicted as follows:

Step 1. Replace $h_1 \sim h_5$ with $h_6 \sim h_{10}$ and update the new initial values of system (1).

$$x_1^0 = \mathrm{mod}\left(\frac{h_6}{256} + \frac{b}{2 \times 255} + t_1, 1\right) \tag{13}$$

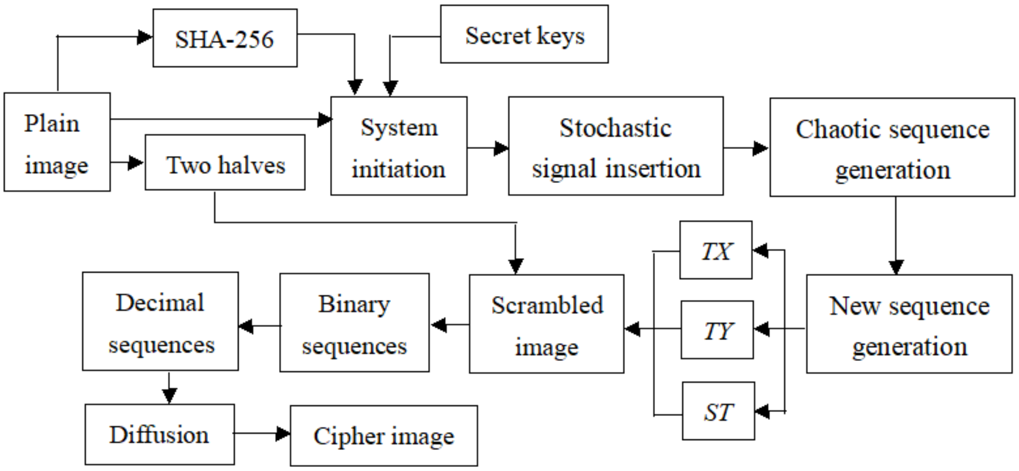


FIGURE 5. Diagram of the proposed image encryption scheme.

$$x_j^0 = \mathrm{mod}\left(\frac{h_{j+5}}{256} + x_{j-1}^0 + t_j, 1\right) \quad (j = 2, 3, 4, 5) \tag{14}$$

Step 2. Generate new sequences $x_1^{'}, x_2^{'}, x_3^{'}, x_4^{'}$ and $x_5^{'}$ with length MN as Step 1 and Step 2 in Section IV.

Step 3. Generate new sequences u and v.

$$u = \mathrm{mod}(floor(abs(x_1^{'} + x_2^{'}) \times 10^{15}), 8) \tag{15}$$

$$v = \mathrm{mod}(floor(abs(x_3^{'} + x_4^{'}) \times 10^{15}), 256) \tag{16}$$

where u and v are integers, and $u \in [0, 7]$, $v \in [0, 255]$.

Step 4. Transform the scrambled image SI into a sequence SC with length MN from the upper-left corner to lower-right corner.

Step 5. Convert the sequences SC and u into their corresponding binary sequences.

Step 6. Obtain sequence SB by Eq. (17).

$$SB(q) = \mathrm{CFT}[SC(q), LSB(u(q)), u(q)] \tag{17}$$

where $\mathrm{CFT}[i, j, l]$ represents the l-bit cyclic shift on the binary sequences i. $LSB(l)$ represents the least significant bit of l. The right cyclic shift or left cyclic shift is decided by $j = 1$ or $j = 0$, and $q = 1, 2, \ldots, MN$.

Step 7. The binary sequence SB is converted into its decimal sequence SD.

Step 8. The diffusion sequence D is achieved as Eq. (18), as shown at the bottom of this page.

where D_i, D_{i-1}, k_{31}, k_{32}, $v(i)$ and $SD(i)$ respectively denote the output cipher-pixel, the previous cipher-pixel, hash value, chaotic sequence value and the scramble sequence value.

Step 9. Transform sequence D into a two-dimensional matrix IE with size $M \times N$. Finally, obtain cipher image IE.

D. IMAGE DECRYPTION

Image decryption is the inverse process of image encryption, and it is briefly explained as follows.

Step 1. Based on given secret keys, generate the chaotic sequences u and v.

Step 2. Obtain sequence SD by Eq. (19), as shown at the bottom of this page.

Step 3. Obtain binary sequence SB based on decimal sequence SD.

Step 4. Obtain sequence SC as Eq. (20).

$$SC(q) = \mathrm{CFT}[SB(q), -LSB(u(q)), u(q)] \tag{20}$$

Step 5. Transform sequence SC into scrambled image SI with size $M \times N$.

Step 6. Produce chaotic sequences and generate TX, TY and ST.

Step 7. Swap pixels in each subimage.

if $ST(i, j) = 0$, exchange $I_1(TX(i, j), TY(i, j))$ with $I_1(i, j)$ and exchange $I_2(TX(i, j), TY(i, j))$ with $I_2(i, j)$;

if $ST(i, j) = 1$, exchange $I_2(TX(i, j), TY(i, j))$ with $I_1(i, j)$ and exchange $I_1(TX(i, j), TY(i, j))$ with $I_2(i, j)$.

Step 8. Connect I_1 and I_2 to form plain image I.

$$D_i = \begin{cases} \mathrm{mod}(SD(i) + v(i), 256) \oplus \mathrm{mod}(k_{31} + v(i), 256) \oplus k_{32} & if\ i = 1 \\ \mathrm{mod}(SD(i) + v(i), 256) \oplus \mathrm{mod}(D_{i-1} + v(i), 256) \oplus v(i) & if\ i = 2 \\ \mathrm{mod}(SD(i) + v(i), 256) \oplus \mathrm{mod}(D_{i-1} + v(i), 256) \oplus D_{i-2} & if\ i \in [3, MN] \end{cases} \tag{18}$$

$$SD_i = \begin{cases} \mathrm{mod}((D_i \oplus \mathrm{mod}(D_{i-1} + v(i), 256) \oplus D_{i-2}) - v(i), 256) & if\ i \in [MN, 3] \\ \mathrm{mod}((D_i \oplus \mathrm{mod}(D_{i-1} + v(i), 256) \oplus v(i)) - v(i), 256) & if\ i = 2 \\ \mathrm{mod}((D_i \oplus \mathrm{mod}(k_{31} + v(i), 256) \oplus k_{32}) - v(i), 256) & if\ i = 1 \end{cases} \tag{19}$$

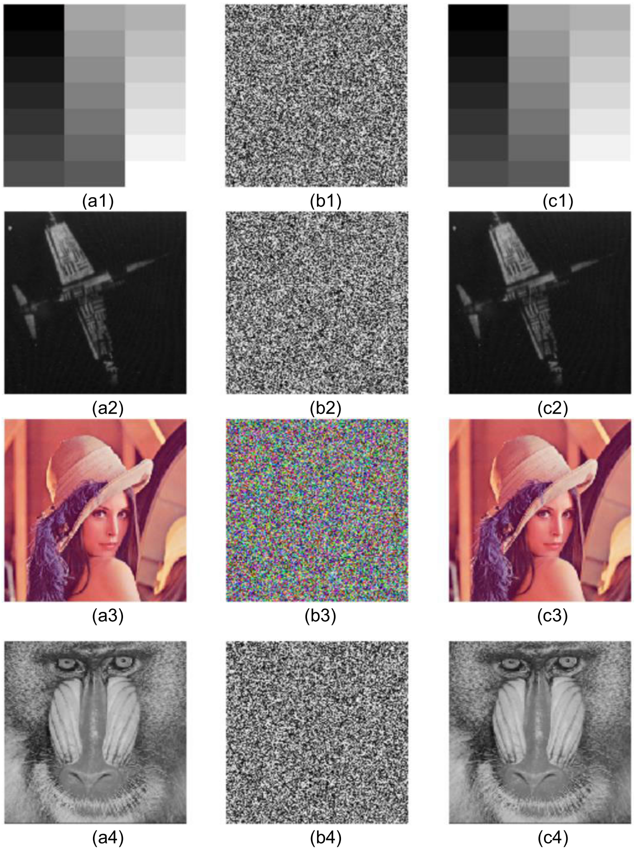


FIGURE 6. Encryption and decryption effects: (a) Plain image, (b) Encrypted image of (a), (c) Decrypted image of (b).

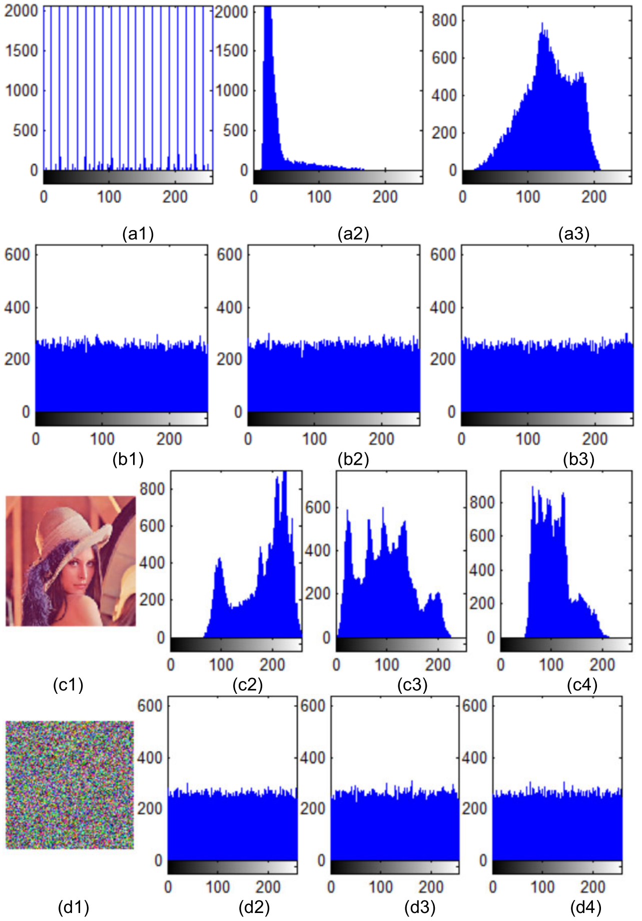


FIGURE 7. The histograms of plain images and corresponding ciphered images: (a) Histogram of grayscale plain image, (b) Histogram of ciphered image of (a), (c) Color image lena and histograms of three components R, G and B, (d) Histogram of cipher of (c).

IV. EXPERIMENTAL RESULTS

MATLAB R2010b is adopted to perform the image encryption and decryption processes of the proposed scheme. The personal computer has a 1.8 GHz CPU, 8G of memory and the Windows 10 operating system. Plain images are grayscale and color images with size 256×256. Secret keys are assigned as follows: $t_1 = 2.4385$, $t_2 = 1.6492$, $t_3 = 0.6358$, $t_4 = 4.7128$, $t_5 = 2.3761$, $\delta_{x_1} = -2.5574$, $\delta_{x_2} = 3.5368$, $\delta_{x_3} = 1.0953$ and $a = 138$. The plain image, encrypted image and corresponding decrypted image are shown in Fig. 6, and histograms of the plain image and corresponding encrypted image are displayed in Fig. 7.

As shown in Figs. 6(b1, b2, b3 and b4), the encrypted images are all noise-like and unrecognizable. It can also be seen in Figs. 7(b and d) that the distributions of the pixel values are very uniform and flat. Attackers cannot identify any relevant information from the encrypted image and its corresponding histogram about the plain image. From Figs. 6(c1, c2, c3 and c4), it can also be concluded that the deciphered images are exactly the same as the plain images.

V. SYSTEM EVALUATION

A. KEY SPACE ANALYSIS

If the key space is larger than 2^{100}, then the cryptosystem can effectively resist an exhaustive attack [46]. In the proposed scheme, the secret keys are composed of: (1) the 256-bit hash value K; (2) the given initial values t_i, where $i = 1, 2, \ldots, 5$; (3) δ_{x_1}, δ_{x_2}, δ_{x_3} and a. If the accuracy of a double-precision number is 10^{-15} [47], the key space is approximately $2^{256} \times (10^{15})^8 \times 256 \approx 2^{256} \times 2^{398} \times 2^8 = 2^{662}$. Therefore, the key space of our scheme is large enough to defend brute-force attacks. The key space comparison results of different schemes are displayed in Table 1.

TABLE 1. Key space comparison results.

Method	Proposed	Ref. [26]	Ref. [29]	Ref. [35]	Ref. [43]
Key space	2^{662}	2^{221}	2^{300}	2^{256}	2^{232}

It can be seen from Table 1 that the proposed scheme has a larger key space than those of [26], [29], [35], [43].

B. KEY SENSITIVE ANALYSIS

A secure image cryptosystem should be sensitive to the secret keys both in the encryption and decryption processes.

The 256-bit hash value is generated from the plain image. Even though there is a one-bit difference between the

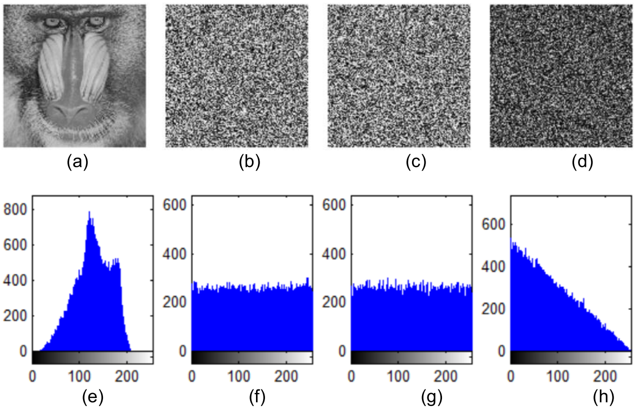


FIGURE 8. **Encrypted images and their histograms with different hash values: (a) Plain image baboon, (b) Ciphered image with K, (c) Ciphered image with K_1, (d) |b-c|, (e) Histogram of (a), (f) Histogram of (b), (g) Histogram of (c), (h) Histogram of (d).**

two images, the produced hash values are totally different. In addition, the initial values of the chaotic system are completely different. The Baboon image (as Fig. 6(a4)) is chosen as an example to demonstrate the encryption and decryption effects. The corresponding encrypted and decrypted images are respectively shown as Figs. 6(b4) and (c4). The initial values are a small modification (10^{-15}), and one bit of hash value K is altered to obtain K_1. K and K_1 are displayed as follows:

$$K = [\underline{7}\,D\,1\,2\,F\,2\,2\,F\,6\,C\,9\,7\,8\,3\,E\,9\,3\,0\,E\,D\,B\,D\,9\,3\,D\,5\,7\,B\,5\,8\,C\,B\,C\,A\,7\,B\,E\,9\,9\,4\,2\,1\,5\,E\,6\,0\,E\,E\,7\,0\,7\,F\,C\,2\,0\,2\,A\,B\,C\,2\,5\,F\,2\,B]$$

$$\mathrm{K}_1 = [\underline{6}\,D\,1\,2\,F\,2\,2\,F\,6\,C\,9\,7\,8\,3\,E\,9\,3\,0\,E\,D\,B\,D\,9\,3\,D\,5\,7\,B\,5\,8\,C\,B\,C\,A\,7\,B\,E\,9\,9\,4\,2\,1\,5\,E\,6\,0\,E\,E\,7\,0\,7\,F\,C\,2\,0\,2\,A\,B\,C\,2\,5\,F\,2\,B]$$

One of the secret keys is modified, and the others remain unchanged during each encryption and decryption processes. The revised secret keys are adopted to encrypt and decrypt images, as shown in Figs. (8)–(10).

It can be seen from Figs. 8 and 9 that even if the secret keys have only a small modification, the encrypted images are totally different. It can also be seen in Fig. 10 that the plain image is correctly decrypted with only the correct secret keys. When the secret keys have a very small alteration, it is impossible to decrypt the correct image. The pixels are changed almost 99.6% between the original image and the decrypted image with improper secret keys.

C. CORRELATION ANALYSIS

The correlation between adjacent pixels in the plain image and the cipher image is researched. It can be calculated as

$$r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{21}$$

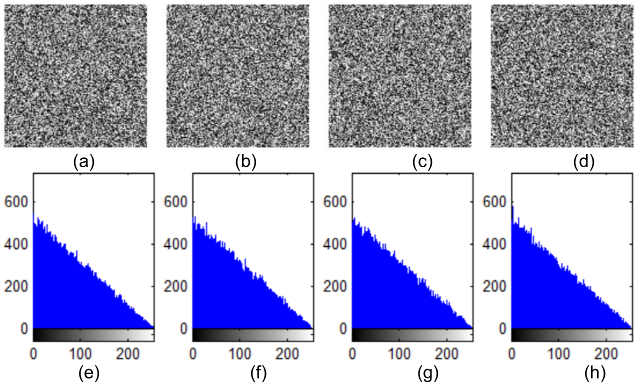


FIGURE 9. **Encryption images and their histograms with different initial values: (a) Encrypted image with $t_1 + 10^{-15}$, (b) Encrypted image with $t_3 + 10^{-15}$, (c) Encrypted image with $\delta_{x_1} - 10^{-15}$, (d) Encrypted image with $\delta_{x_3} + 10^{-15}$, (e) |Fig. 8(b) - Fig. 9(a)|, (f) |Fig. 8(b) - Fig. 9(b)|, (g) |Fig. 8(b) – Fig. 9(c)| and (h)| Fig. 8(b) - Fig. 9(d)|.**

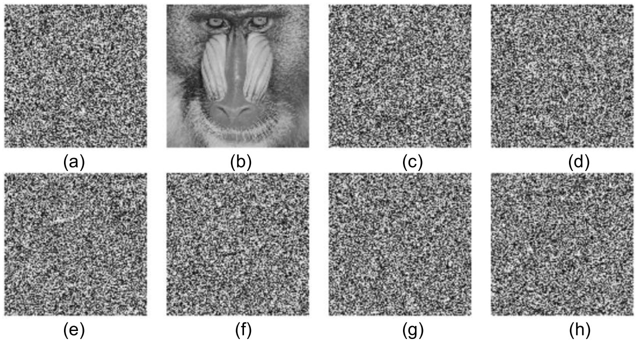


FIGURE 10. **Decryption images with different initial values: (a) Encrypted image, (b) Right decrypted result, (c) Decrypted result with K_1, (d) Decrypted result with $t_2 - 10^{-15}$, (e) Decrypted result with $t_4 + 10^{-15}$, (f) Decrypted result with $t_5 + 10^{-15}$, (g) Decrypted result with $\delta_{x_1} - 10^{-15}$, and (h) Decrypted result with $\delta_{x_2} + 10^{-15}$.**

where

$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),$$
$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i, \quad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{22}$$

here x_i and y_i are adjacent pixels, and N is the total number of pixel pairs.

Two thousand pairs of adjacent pixels are randomly selected from the plain and corresponding encrypted images in four (horizontal, vertical, diagonal and counter diagonal) directions. Figure 11 displays the correlation of adjacent pixels in the plain image Baboon and corresponding encrypted image. It can be seen that the correlation of adjacent pixels is high in the plain image, but it is extremely low in the encrypted image.

Correlation coefficients of the cipher image are listed in Table 2, and Table 3 shows the comparison results.

From Fig. 11 and Table 2, it can be seen that the correlation of the plain image is very strong, and that of the cipher image

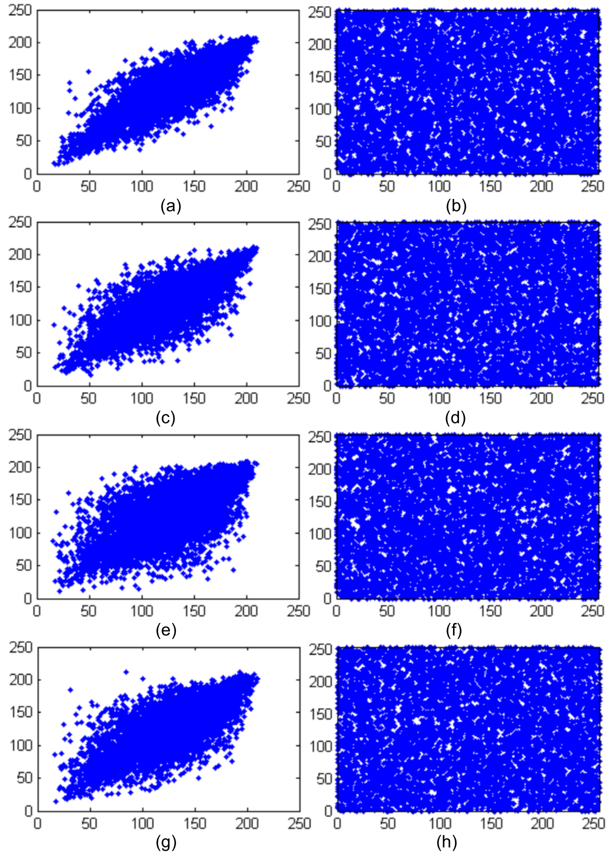


FIGURE 11. Distribution of adjacent pixels in the baboon image and corresponding ciphered image: (a), (c), (e), (g) are horizontal, vertical, diagonal and counter diagonal direction of plain image, and (b), (d), (f), (h) are horizontal, vertical, diagonal and counter diagonal direction of corresponding ciphered image.

TABLE 2. Correlation coefficients of cipher images.

Image		Horizontal	Vertical	Diagonal	Counter diagonal
Band		-0.0076	-0.0077	-0.0060	0.0157
Plane		0.0009	-0.0097	-0.0031	0.0086
Lena	R	-0.0007	0.0015	-0.0039	0.0019
	G	0.0037	0.0025	0.0088	-0.0036
	B	0.0012	-0.0062	-0.0086	0.0021
Baboon		0.0031	0.0028	0.0039	0.0052

is very weak. It can also be seen from Table 3 that the proposed scheme has smaller absolute correlation coefficients than the methods in Refs. [29], [49] in four directions, and the encryption effect is much better than those in [26], [43] in three directions. Thus, the proposed scheme can effectively resist correlation analysis attack.

D. HISTOGRAM ANALYSIS

A histogram reveals the intensity of pixel values about the image. Figure 7 displays the histograms of plain and corresponding encrypted images. It can be seen that the cipher images have a uniform histogram and can effectively defend statistical analysis. The Chi-square test [48], [49] is used to measure the uniformity of the histogram. It is defined as

TABLE 3. Correlation coefficients comparison in the baboon image.

Scheme	Horizontal	Vertical	Diagonal	Counter diagonal
Baboon	0.8792	0.8336	0.7917	0.6943
Ref. [26]	0.0054	0.0004	0.0044	-0.0068
Ref. [29]	-0.0122	-0.0032	0.0406	0.0153
Ref. [43]	-0.0039	0.0012	-0.0043	-0.0206
Ref. [49]	-0.0035	0.0031	-0.0028	0.0159
Proposed	0.0031	0.0028	0.0039	0.0052

TABLE 4. Chi-square test of histogram.

Image	Band	Plane	Lena	Baboon
$\chi^2_{0.05}(255)$	293.25	293.25	293.25	293.25
χ^2_{test}	235.25	275.41	249.26	242.41
Decision	Pass	Pass	Pass	Pass

$$\chi^2 = \sum_{i=1}^{256} \frac{(o_i - e_i)^2}{e_i} \tag{23}$$

$$e_i = \frac{M \times N}{256} \tag{24}$$

where o_i and e_i represent the actual and expected frequency of each gray level. If the significance level is 0.05, and the scores of χ^2_{test} are smaller than $\chi^2_{0.05}(255) = 293.25$ [49], then the null hypothesis is accepted, and the distribution of the histogram is considered uniform. Chi-square results are presented in Table 4 for different cipher images.

It can be seen from Table 4 that all scores generated by the proposed method are lower than the theoretical value 293.25. Therefore, it can be considered that the distribution of histogram is uniform, and the proposed scheme passes the Chi-square test.

E. INFORMATION ENTROPY ANALYSIS

Global Shannon entropy is widely used to measure the randomness of an information source, and it is defined as Eq. (25).

$$H(m) = -\sum_{i=1}^{256} p(m_i) \log_2 p(m_i) \tag{25}$$

where m_i represents the ith message source and $p(m_i)$ is the probability of m_i. The ideal entropy for an 8-bit grayscale

TABLE 5. Global and local entropy.

Image	Global entropy	Local entropy	Local entropy critical value k=30, $T_B^{L=256*}$=1936		
			$h_{left}^{l*0.001}=7.9015$ $h_{right}^{l*0.001}=7.9034$	$h_{left}^{l*0.01}=7.9017$ $h_{right}^{l*0.01}=7.9032$	$h_{left}^{l*0.05}=7.9019$ $h_{right}^{l*0.05}=7.9030$
			0.001-level	0.01-level	0.05-level
Band	7.9974	7.9020	pass	pass	pass
Plane	7.9970	7.9028	pass	pass	pass
Lena(R)	7.9973	7.9023	pass	pass	pass
Lena(G)	7.9970	7.9020	pass	pass	pass
Lena(B)	7.9974	7.9023	pass	pass	pass
Baboon	7.9973	7.9031	pass	pass	no

TABLE 6. NPCR and UACI values for different methods.

Method	Criteria	Band	Plane	Lena	Baboon
Proposed	NPCR (%)	99.62	99.59	99.61	99.61
	UACI (%)	33.50	33.45	33.46	33.48
Ref. [29]	NPCR (%)	99.64	99.63	99.65	99.64
	UACI (%)	33.52	33.43	33.56	33.51
Ref. [26]	NPCR (%)	99.62	99.59	99.61	99.60
	UACI (%)	33.47	33.42	33.48	33.45
Ref. [49]	NPCR (%)	99.63	99.62	99.58	99.59
	UACI (%)	33.52	33.46	33.50	33.47

image is 8. However, the global Shannon entropy cannot exactly reflect the true randomness for some weaknesses [50]. The local Shannon entropy (*LSE*) was proposed by Wu *et al.* [50] and was employed to measure the randomness of encrypted image. The (k, T_B) *LSE* can be defined as Eq. (26).

$$\overline{H_{k,T_B}}(S)=\sum_{i=1}^{k}\frac{H(S_i)}{k} \tag{26}$$

where S_i $(i = 1, 2, \ldots, k)$ is an arbitrarily chosen and non-overlapping image block with T_B pixels from a ciphered image. $H(S_i)$ represents the global information entropy of image block S_i and $(k, T_B) = (30, 1936)$ is selected in this paper. If the value of *LSE* belongs to the interval $[h_{left}^{l*\alpha}, h_{right}^{l*\alpha}]$, then it passes the test and has very high randomness [26]. The values of global and local entropy for ciphered images are listed in Table 5.

It can be seen from Table 5 that global information entropy is close to the ideal value 8. All local entropies pass the test at 0.001 and 0.01 significance levels; only one does not pass the test at 0.05 significance level. From Table 5, it can be concluded that the randomness of the proposed scheme is very high, and it can resist entropy analysis.

F. DIFFERENTIAL ATTACK ANALYSIS

The number of pixel changing rate (NPCR) and unified average changed intensity (UACI) are often used to measure the ability to defend differential attacks [13]. They are defined by (27)–(29).

$$NPCR=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times 100\% \tag{27}$$

$$UACI=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\times 100\% \tag{28}$$

$$D(i,j)=\begin{cases}0, & if\ C_1(i,j)=C_2(i,j)\\ 1, & else\end{cases} \tag{29}$$

where C_1 and C_2 respectively represent the ciphered images before and after modifying one pixel in the plain image.

Wu *et al.* [52] proposed a new hypothesis about NPCR and UACI. The critical values NPCR* and UACI* with α significance level are defined as (30) and (31).

$$NPCR_\alpha^{*}=(F-\Phi^{-1}(\alpha)\sqrt{F/MN})/(F+1) \tag{30}$$

$$\begin{cases}UACI_\alpha^{*-}=\dfrac{F+2}{3F+3}-\Phi^{-1}(\alpha/2)\\ \qquad\times\sqrt{\dfrac{(F+2)(F^2+2F+3)}{18(F+1)^2MNF}}\\ UACI_\alpha^{*+}=\dfrac{F+2}{3F+3}+\Phi^{-1}(\alpha/2)\\ \qquad\times\sqrt{\dfrac{(F+2)(F^2+2F+3)}{18(F+1)^2MNF}}\end{cases} \tag{31}$$

TABLE 7. NPCR randomness test.

Image	NPCR value (%)	Theoretical NPCR critical value [52]		
		$N^*_{0.001}$ = 99.5341%	$N^*_{0.01}$ = 99.5527%	$N^*_{0.05}$ =99.5693%
		0.001-level	0.01-level	0.05-level
Band	99.63	pass	pass	pass
Plane	99.58	pass	pass	pass
Lena	99.61	pass	pass	pass
Baboon	99.61	pass	pass	pass

TABLE 8. UACI randomness test.

Image	UACI value (%)	Theoretical UACI critical value [52]		
		$UACI^{*-}_{0.001}$ =33.1594% $UACI^{*+}_{0.001}$ = 33.7677%	$UACI^{*-}_{0.01}$ =33.2255% $UACI^{*+}_{0.01}$ = 33.7016%	$UACI^{*-}_{0.05}$ =33.2824% $UACI^{*+}_{0.05}$ =33.6447%
		0.001-level	0.01-level	0.05-level
Band	33.60	pass	pass	pass
Plane	33.45	pass	pass	pass
Lena	33.36	pass	pass	pass
Baboon	33.50	pass	pass	pass

TABLE 9. PSNR values of different schemes with different percentages of salt & pepper noise (dB).

Method	Noise density					
	0.0001	0.0005	0.001	0.005	0.01	0.05
Ref. [35]	41.40	34.17	30.93	24.03	21.18	14.32
Ref. [36]	9.52	8.93	8.62	8.56	8.55	8.55
Ref. [49]	42.69	36.84	31.53	28.71	9.29	18.84
Proposed	62.69	56.79	53.99	47.82	44.57	37.46

where F is the maximum pixel value, and $\Phi^{-1}(\alpha)$ represents the inverse cumulative density function of a standard normal distribution.

When the value of NPCR>NPCR*, it passes the test. UACI passes the randomness test if it falls into the interval $[UACI^{*-}, UACI^{*+}]$. The ideal values of NPCR and UACI are 99.609375% and 33.463541% [51]. The values of NPCR and UACI with different methods are given in Table 6. NPCR and UACI randomness tests are displayed in Table 7 and 8.

From Table 6, it can be seen that the NPCR and UACI of the proposed scheme are very close to the ideal value. It can also be concluded from Table 7 and Table 8 that all images pass the NPCR and UACI tests. Therefore, the proposed scheme can effectively resist differential attack.

G. NOISE AND DATA LOSS ANALYSIS

When an encrypted image is blurred with noise or loses some data during transmission, an effective image encryption scheme should be able to reconstruct the plain image with high visual effect.

The encrypted image is blurred by Salt & Pepper noise with densities of 0.001, 0.01, 0.05 and 0.1, and the corresponding decrypted images are shown in Figs. 12(a)-(d).

It can be seen from Fig. 12 that all the recovered results can be recognized, which means that the cipher data with noise is tolerable.

As shown in Figs. 13a-d, the cipher image loses 1/32, 1/16, 1/8 and 1/4 data, and the corresponding decrypted images are displayed in Figs. 13(e)-(h). These results

TABLE 10. PSNR values of different schemes with different percentages of data loss (dB).

Method	Data loss				
	1/32	1/16	1/8	1/4	1/2
Ref. [35]	20.76	18.51	15.93	11.15	8.72
Ref. [36]	8.615	8.568	8.554	8.550	8.548
Ref. [49]	24.37	20.63	17.64	14.61	11.61
Proposed	42.15	39.43	36.55	33.53	30.50

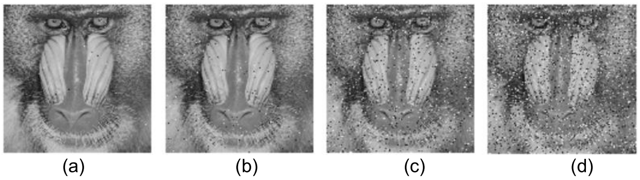


FIGURE 12. Recovered image under salt & pepper noise with densities of (a) 0.001, (b) 0.01, (c) 0.05, (d) 0.1.

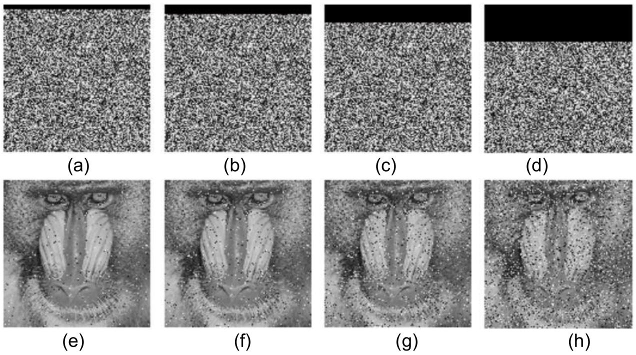


FIGURE 13. Data loss attack analysis results: (a) 1/32 data loss, (b) 1/16 data loss, (c) 1/8 data loss, (d) 1/4 data loss, (e) Decrypted image of (a), (f) Decrypted image of (b), (g) Decrypted image of (c), (h) Decrypted image of (d).

demonstrate that the proposed scheme can resist the given data loss attacks.

The peak signal-to-noise ratio (*PSNR*) is used to measure the ability to resist noise and data loss [35]. It is adopted to measure the difference between plain image I and the decrypted image I'. It is defined as follows:

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}} \tag{32}$$

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(I_{ij} - I'_{ij} \right)^2 \tag{33}$$

The value of PSNR is higher, and the difference between I and I' is smaller. The results are shown in Table 9 and Table 10.

It is clear that the proposed method provides higher PSNR values than those in [35], [36], [49] when images are decrypted under noise and occlusion attacks. Therefore, the proposed scheme is superior to the comparative methods.

TABLE 11. Computational complexity analysis of the proposed scheme.

	Computational complexity		
	Permutation	Diffusion	Total
Addition	13.5*MN*+20	19*MN*+10	32.5*MN*+30
Multiplication	4.5*MN*+6	9*MN*+16	13.5*MN*+22
Mod	2*MN*+15	8*MN*+5	10*MN*+20
Absolute value	4*MN*	2*MN*	6*MN*
XOR	10	6*MN*	6*MN*+10
Floor function	*MN*	2*MN*	3*MN*
Comparison	2*MN*	0	2*MN*
Cycle shift	0	*MN*	*MN*

TABLE 12. Computational complexity of different schemes.

Method	Complexity order	Order of magnitude
Ref. [35]	$O(40MN)$	2.6×10^6
Ref. [36]	$O(180MN)$	11.8×10^6
Ref. [49]	$O(124MN)$	8.1×10^6
Proposed	$O(74MN)$	4.8×10^6

H. COMPLEXITY ANALYSIS

Complexity is another important index for cryptosystem. In our scheme, Table 11 reveals the computational complexity of the proposed scheme. Different schemes are compared in Table 12 for a 256 × 256 grayscale image.

It can be seen from Table 11 and 12 that the proposed algorithm is the second-fastest in the four methods, which means that the proposed scheme is efficient.

VI. CONCLUSION

A novel chaotic encryption scheme is proposed in this paper. A 5D hyperchaotic system is applied to generate pseudorandom numbers for permutation and diffusion.

The SHA-256 hash function is employed to enhance the sensitivity to plain image. Stochastic signal insertion enlarges the key space and increases the dynamic behavior of the cryptosystem. The plain image is equally divided into two halves when scrambling. An X-coordinate, a Y-coordinate and a control table are constructed based on generated pseudonumber sequences. Pixel scrambling is determined by the value of the control table. Cyclic shift is employed during the diffusion process. Security and performance analyses are performed to verify the effect of the proposed algorithm. It is proven that the cryptosystem has a large key space, high sensitivity to plain image and secret keys, little adjacent pixel correlation, and ideal global and local Shannon entropy. Moreover, the cryptosystem has low computational complexity, and can effectively defend statistical attacks, differential attacks, noise and data loss attacks.

REFERENCES

[1] S. H. Soleymani and A. H. Taherinia, "High capacity image steganography on sparse message of scanned document image (SMSDI)," *Multimed. Tools Appl.*, vol. 76, no. 20, pp. 20847–20867, Oct. 2017.

[2] A. Girdhar and V. Kumar, "Comprehensive survey of 3D image steganography techniques," *IET Image Process.*, vol. 12, no. 1, pp. 1–10, Jan. 2018.

[3] C. Vanmathi and S. Prabu, "Image steganography using fuzzy logic and chaotic for large payload and high imperceptibility," *Int. J. Fuzzy Syst.*, vol. 20, no. 2, pp. 460–473, 2018.

[4] X. Liu, G. Han, J. Wu, Z. Shao, G. Coatrieux, and H. Shu, "Fractional Krawtchouk transform with an application to image watermarking," *IEEE Trans. Signal Process.*, vol. 65, no. 7, pp. 1894–1908, Apr. 2017.

[5] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3669–3697, 2017.

[6] C.-P. Wang, X.-Y. Wang, and Z.-Q. Xia, "Geometrically invariant image watermarking based on fast radial harmonic Fourier moments," *Signal Process.-Image*, vol. 45, pp. 10–23, Jul. 2016.

[7] G. Hua, L. Zhao, H. Zhang, G. Bi, and Y. Xiang, "Random matching pursuit for image watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 3, pp. 625–639, Mar. 2019.

[8] M. Brindha and N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem," *Appl. Soft Comput.*, vol. 40, pp. 379–390, Mar. 2016.

[9] X. Wang, Y. Zhang, and L. Liu, "An enhanced sub-image encryption method," *Opt. Laser. Eng.*, vol. 86, pp. 248–254, Nov. 2016.

[10] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Opt. Lasers Eng.*, vol. 90, pp. 146–154, Mar. 2017.

[11] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 60, pp. 12–32, Jul. 2018.

[12] X. Li, Z. Xie, J. Wu, and T. Li, "Image encryption based on dynamic filtering and bit cuboid operations," *Complexity*, vol. 2019, Jan. 2019, Art. no. 7485621.

[13] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016.

[14] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, Jan. 2018.

[15] D. Huo, D.-F. Zhou, S. Yuan, S. Yi, L. Zhang, and X. Zhou, "Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding," *Phys. Lett. A*, vol. 383, no. 9, pp. 915–922, Feb. 2019.

[16] X.-D. Chen, Q. Liu, J. Wang, and Q.-H. Wang, "Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction," *Opt. Laser. Technol.*, vol. 107, pp. 302–312, Nov. 2018.

[17] Z. Chen, X. Hou, X. Qian, and C. Gong, "Efficient and robust image coding and transmission based on scrambled block compressive sensing," *IEEE Trans. Multimedia*, vol. 20, no. 7, pp. 1610–1621, Jul. 2018.

[18] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Process.*, vol. 155, pp. 218–232, Feb. 2019.

[19] L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, "A novel image encryption scheme based on nonuniform sampling in block compressive sensing," *IEEE Access*, vol. 7, pp. 22161–22174, 2019.

[20] Y. Wei, A. Yan, J. Dong, Z. Hu, and J. Zhang, "Optical image encryption using QR code and multilevel fingerprints in gyrator transform domains," *Opt. Commun.*, vol. 403, pp. 62–67, Nov. 2017.

[21] Y. Qin, Z. Wang, H. Wang, and Q. Gong, "Binary image encryption in a joint transform correlator scheme by aid of run-length encoding and QR code," *Opt. Laser. Technol.*, vol. 103, pp. 93–98, Jul. 2018.

[22] P. Zhu, W. Xu, and Y. Shi, "High-capacity encryption system based on single-shot-ptychography encoding and QR code," *Opt. Commun.*, vol. 435, pp. 426–432, Mar. 2019.

[23] H.-M. Yuan, Y. Liu, T. Lin, T. Hu, and L.-H. Gong, "A new parallel image cryptosystem based on 5D hyper-chaotic system," *Signal Process., Image Commun.*, vol. 52, pp. 87–96, Mar. 2017.

[24] A. A. A. El-Latif, L. Li, and X. Niu, "A new image encryption scheme based on cyclic elliptic curve and chaotic system," *Multimed. Tools Appl.*, vol. 70, no. 3, pp. 1559–1584, Jun. 2014.

[25] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 407–425, Jan. 2017.

[26] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.

[27] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

[28] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[29] 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, pp. 41–52, Apr. 2017.

[30] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.

[31] Z. Wu, X. Zhang, and X. Zhong, "Generalized chaos synchronization circuit simulation and asymmetric image encryption," *IEEE Access*, vol. 7, pp. 37989–38008, 2019.

[32] S. Sun, Y. Guo, and R. Wu, "A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping," *IEEE Access*, vol. 7, pp. 28539–28547, 2019.

[33] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13681–13701, 2017.

[34] X. Li, Y. Wang, and Q.-H. Wang, "Modified integral imaging reconstruction and encryption using an improved SR reconstruction algorithm," *Opt. Lasers Eng.*, vol. 112, pp. 162–169, Jan. 2019.

[35] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018.

[36] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.

[37] 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, 2015.

[38] C. Han, Y. Shen, and W. Ma, "Iteration and superposition encryption scheme for image sequences based on multi-dimensional keys," *Opt. Commun.*, vol. 405, pp. 101–106, Dec. 2017.

[39] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, Apr. 2018, Art. no. 7201714.

[40] W. Feng and Y.-G. He, "Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling," *IEEE Photon. J.*, vol. 10, no. 6, Dec. 2018, Art. no. 7909215.

[41] H.-I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Process.*, vol. 117, pp. 281–309, Dec. 2015.

[42] H. Fan, M. Li, D. Liu, and E. Zhang, "Cryptanalysis of a colour image encryption using chaotic APFM nonlinear adaptive filter," *Signal Process.*, vol. 143, pp. 28–41, Feb. 2018.

[43] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[44] 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.

[45] A. Kadir, M. Aili, and M. Sattar, "Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections," *Optik*, vol. 129, pp. 231–238, Jan. 2017.

[46] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[47] *IEEE Standard for Floating-Point Arithmetic*. IEEE Standard 754-2008, Aug. 1985.

[48] 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.

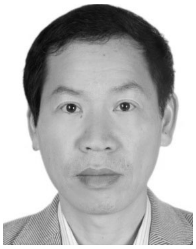
[49] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.

[50] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

[51] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimed. Tools Appl.*, vol. 76, no. 5, pp. 6229–6245, 2017.

[52] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, Apr. 2011.

SHULIANG SUN received the B.S. degree in measuring and controlling technology and instrument from Hangzhou Dianzi University, in 2003, the M.S. degree in electrical engineering from Guangxi University, in 2006, and the Ph.D. degree in pattern recognition and intelligent system from Tongji University, in 2011. Since 2014, he has been an Associate Professor with the College of Computer Science and Technology, Fuqing Branch of Fujian Normal University. His research interests include information security, image processing, and pattern recognition.



YONGNING GUO received the B.S. degree from Mathematics Department, Fujian Normal University, in 1989, and the M.S. degree from Software College, University of Electronic Science and Technology of China, in 2012. Since 2013, he has been a Professor with the College of Computer Science and Technology, Fuqing Branch of Fujian Normal University. His research interests include algorithm design and analysis, image processing, and pattern recognition.

RUIKUN WU received the B.S. degree in electronics and communication engineering from Radio Engineering Department, Fuzhou University, in 1987, and the M.S. degree in communication and information system from Fuzhou University, in 2007. From 2009 to 2010, he was a Visiting Scholar with Tongji University. Since 2014, he has been a Professor with the Electronic Information Engineering, Fuqing Branch of Fujian Normal University. His research interests include technology of electronics, image processing, and power electronic technology.