IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 11, 2019, accepted May 30, 2019, date of publication June 6, 2019, date of current version June 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2921309

A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals

XUNCAI ZHANG, (Member, IEEE), LINGFEI WANG, ZHENG ZHOU, AND YING NIU
School of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

Corresponding author: Ying Niu (niuying@zzuli.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602424 and Grant 61572446, in part by the Plan for Scientific Innovation Talent of Henan Province under Grant 192102210134, and in part by the Key Scientific Research Projects of Henan High Educational Institution under Grant 18A510020.

ABSTRACT Image encryption is the most direct and effective technical means for protecting the security of image information. Based on the space filling property of the Hilbert curve and the infinite property of the H-geometric fractal, a new image encryption technique is proposed, which combines the pseudo-randomness of a hyperchaotic system and the sensitivity to initial values. First, the hash value of a plaintext image is calculated using the secure hash algorithm 3 (SHA-3) as the initial value of the piece-wise linear chaotic map (PWLCM) and Rossler chaotic systems, which associates the key with the plaintext. In addition, the chaotic sequences that are generated by the chaotic systems are used to scramble the global pixel positions and the pixel values of the images, thereby disturbing the distribution of the pixel positions and the pixel values. Second, the Hilbert curve and H-fractal are alternately used to scramble the local pixel positions and diffuse the pixel values twice. Finally, the ciphertext feedback is used to further enhance the confusion and diffusion characteristics of the algorithm in order to achieve higher security. The experimental results and security analysis show that the encryption technique has enough key space to resist exhaustive attacks and can effectively resist statistical attacks, differential attacks, noise attacks, and cropping attacks. It can be used for military, judicial, and other privacy-related digital images secure storage and network security transmissions.

INDEX TERMS Hilbert curve, H-geometric fractal, hyperchaotic system, SHA-3, image encryption, chaotic cryptography.

I. INTRODUCTION

With the rapid development of Internet technology and multimedia technology, increasingly more attention has been paid to the secure transmission of information such as images, videos, audio and so on [1], [2]. Compared with text data, digital images have the characteristics of large data volumes, strong correlations and high redundancy. Traditional encryption methods such as data encryption standard (DES), triple DES (3DES), and advanced encryption standard (AES) [3], [4] are not suitable for image encryption due to their slow encryption speeds and small key spaces [5], [6].

As a complex nonlinear dynamic system, a chaotic system has the characteristics of sensitivity to the initial values, pseudo-randomness, and unpredictable motion trajectories, which are consistent with the characteristics of cryptography, and thus, it is widely used in image encryption [7]–[10]. In 2004, Chen *et al*. proposed a symmetric image encryption scheme based on the 3D Cat map [11]. The scheme used the 3D Cat map to scramble the positions and pixel values of the image and used the 2D Cat map to confuse the relationship between plaintext images and ciphertext images, which significantly improved the ability of the algorithm to resist statistical attacks and differential attacks. In 2005, Guan *et al.* proposed an image encryption algorithm based on a chaotic system. The algorithm first used the Arnold cat map to scramble the pixel positions of the images in the spatial domain and then used the pseudo-random sequences generated by the Chen chaos to preprocess the discrete chaotic signals so as to realize the scrambling of pixel positions and the synchronous diffusion of pixel values [12]. In 2008, Behnia *et al.* proposed a digital image encryption scheme based on a hybrid chaotic system, which mixed a typical coupling map with a

The associate editor coordinating the review of this manuscript and approving it for publication was Ke Gu.

one-dimensional chaotic map in order to enhance the complexity and security of the algorithm [13]. In 2011, Awad proposed a new method for image encryption using chaotic systems. This method used a two-dimensional chaotic system to scramble the pixel positions of the image and used a piecewise linear chaotic map to permute and diffuse the image over multiple rounds [14]. The experimental results and security analysis show that the algorithm can perform secure and effective real-time image encryption.

However, a single chaotic system has some problems, such as short periods, a limited precision effect and so on. For this reason, a series of image encryption methods combined with chaotic systems have emerged. In 2013, El-Latif *et al.* proposed an image encryption method based on a combination of a cyclic elliptic curve and a chaotic system. The method combined the keys that were generated by the chaotic system with the keys of the cyclic elliptic curve in order to obtain stronger encryption keys and improve the security of the algorithm [15]. In 2014, Wang *et al.* proposed an image encryption method based on a dynamic S-box in which the S-box is composed of a chaotic system. The parameters and initial state of the chaotic system are generated by using the external 256-bit key and the last pixel of the plaintext image as the first S-box. By dividing the plaintext image into several blocks and replacing the pixels with an S-box, the correlation between the adjacent pixels is broken down, which greatly reduces the computational and time complexity [16]. In 2015, Zhou *et al.* proposed a symmetric image encryption algorithm based on the oblique tent map. The algorithm eliminates the limitations of images' length and width and is suitable for the encryption of grayscale images and color images of any size [17]. In 2016, Tang *et al.* proposed an image encryption algorithm that is suitable for multi-gray images. The algorithm decomposed the input image into bit planes, randomly exchanged the bit blocks between different bit planes, and performed an exclusive OR operation between the scrambled image and the key matrix under the control of the chaotic map. The algorithm used multiple keys and improved its security with respect to the batch processing of a high-performance large image database [18]. In 2018, Ping *et al.* proposed an image encryption algorithm based on cellular automata and chaos. The encryption algorithm included two stages of confusion and diffusion. In the confusion stage, the two-dimensional Logistic-adjusted-Sine map was used to scramble the pixel position of the image to reduce the computational complexity. In the diffusion stage, the image pixels were permuted by a second-order cellular automaton. The result of each iteration reversed and undistorted the encryption algorithm [19]. In 2019, Hanis *et al.* proposed a new improved Logistic map based on the extended key space, the integer-based key generation algorithm and the block image encryption algorithm based on the improved Logistic map and butterfly structure. Compared with other encryption algorithms, the algorithm has higher security and faster encryption speed [20].

With the research and development of fractal theory, fractal encryption is favored by scholars as a new research field [21]–[23]. Fractal theory is an important part of nonlinear science, and its mathematical basis is fractal geometry. Fractal geometry has a fine structure of infinite nested levels and has some self-similar characteristics in very small proportions. The characteristics of the fractal geometry determine the natural connection and structural similarity between the fractal geometry and cryptography, which inspires people to apply fractal geometry to the field of cryptography [24]–[26].

Based on this theory, a new image encryption algorithm is proposed based on the H-geometric fractal, the Hilbert curve, and chaotic systems. The algorithm used the hash value of the plaintext image to associate the plaintext with the key. The chaotic sequence, Hilbert curve, and H-geometric fractal of the image are used to scramble and diffuse the image pixels several times to enhance the confusion and diffusion characteristics of the algorithm.

The objective of this paper is to ensure more security over conventional asymmetric cryptosystems using the space filling property of the Hilbert curve and the infinite property of the H-geometric fractal. A novel chaos-based image encryption technique based on the Hilbert curves and H-fractals is proposed. The hash value of a plaintext image is calculated employing the SHA-3 algorithm as the initial value of the chaos systems, and the chaos-generated sequences are applied to scramble the global pixel positions and the pixel values of the images; the Hilbert curve and H-fractal are alternately used to scramble the local pixel positions and diffuse the pixel values twice. Finally, the ciphertext feedback is applied to further enhance the confusion and diffusion characteristics of the algorithm to achieve higher security. Thus the multifold security makes the method more efficient and can be utilized in judicial and other privacy-related image secure storage and network security transmissions.

The remainder of the paper is organized as follows. Basic theories are given in Section II to discuss the Hilbert curves, the H-fractals, and the chaotic systems. In Section III, the pixel scrambling, the pixel diffusion, the ciphertext feedback, and the encryption process are introduced. The experimental results and security analysis are presented in Section IV. Finally, this paper is concluded in Section V.

II. BASIC THEORY

A. HILBERT CURVE

The Italian mathematician Peano and the German mathematician Hilbert gave the FASS curve filling a square grid in 1890 and 1891, respectively [27], [28], and gave a method for traversing each node in the grid using this continuous curve, which is called the Hilbert curve. The Hilbert curve is an FASS curve, that is, space-filling, self-avoiding, self-similar, and simple curve. These curves are located in a Euclidean space with a dimension greater than 1 and have non-empty interiors within the space. Figure 1 shows a path for the Hilbert curve to traverse the grid.

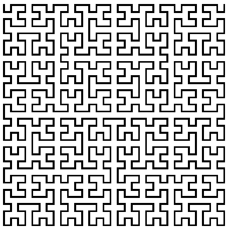


FIGURE 1. The Hilbert curve.

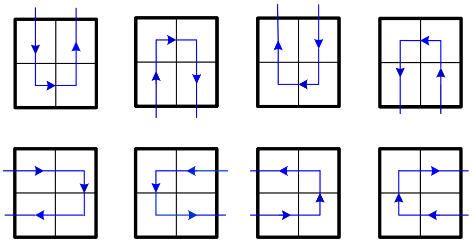


FIGURE 2. Eight different scrambling schemes.

The first-order Hilbert curve can be described as follows: divide a square into four small squares starting from the center of the square in the lower-left corner, then going to the center of the square in the upper-left corner, then going to the center of the square in the upper-right corner, and then going down to the right. After arriving at the center of the square at the bottom corner, this completes the first iteration, and the result is shown in Figure 2(b). The positions of the starting point and the end point of the Hilbert curve determine its direction. In the image, it determines the order in which it traverses the spatial pixels. Therefore, according to the selection and combination of the starting and end points of the Hilbert curve, eight different scrambling schemes can be generated for the first-order Hilbert curve, as shown in Figure 2.

Figure 2(b) is placed in the upper-left and upper-right corners of the 2×2 grid shown in Figure 3(a). Two representations of the Figure 2(b) are rotated 90 degrees clockwise and 90 degrees counterclockwise, respectively, and then placed in the lower-left and lower-right corner regions, respectively. The second iteration curve can be obtained by connecting the adjacent end points of the curve, as shown in Figure 3(a). Figure 3(b) shows the Hilbert curve after three iterations. By repeating the above operations, a two-dimensional Hilbert curve that traverses the entire square grid can be obtained.

B. H-FRACTAL

Fractal Geometry was originally defined as a set by Mandelbrot. Subsequently, Falconer, a British mathematician, defined Fractal Geometry and its calculation methods in his work Fractal Geometry: Mathematical Foundations and Applications in 1990 [29]. Since then, fractal geometry has been widely used in mathematics and physics. The specific characteristics of fractal geometry are as follows:

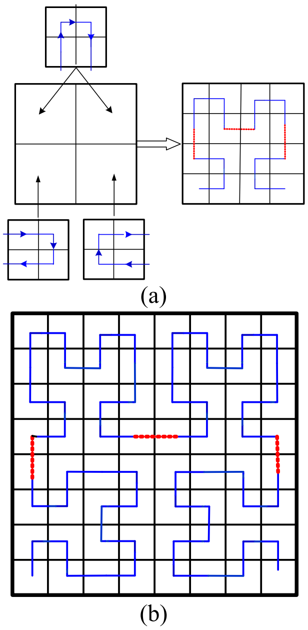


FIGURE 3. The generation process of a two-dimensional Hilbert curve, (a) Hilbert's second iteration curve, (b) two-dimensional Hilbert curve.

(1) Fractal geometry has self-similarity, that is, the whole and part of the fractal have similarity;
(2) Fractal geometry has a complex structure, that is, the non-escape point inside the fractal geometry and the distribution are concentrated and present a complex structure; and
(3) Fractal geometry can usually be composed using simple iterative methods.

In fractal geometry, the common fractals are the H-fractal, the Cantor set, the Koch curve, and the Julia set. The H-fractal is a fractal tree structure composed of vertical line segments, and each line segment is less than the square root of 2 times the next largest adjacent line segment. The Hausdorff dimension is 2, and the H-fractal is arbitrarily close to each point in the rectangle. Its Major applications include information encryption, microwave engineering, and large-scale integrated circuit design.

C. CHAOTIC SYSTEMS

1) PIECE-WISE LINEAR CHAOTIC MAP (PWLCM)

The PWLCM system has gained increasing attention in encryption algorithms because of its less sensitivity towards external perturbation than the conventional Logistic map [30], its simplicity in representation, efficiency in implementation, as well as good dynamical behavior [31]. And the mathematical description of the one-dimensional PWLCM is shown as follows:

$$F(s) = \begin{cases} s/p, & if\ 0 \le s < p \\ (s-p)/(0.5-p), & if\ p \le s < 0.5 \\ 1-s, & if 0.5 \le s < 1, \end{cases} \tag{1}$$

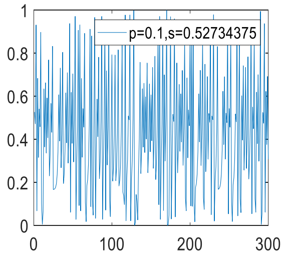


FIGURE 4. Phase diagram of the PWLCM system with p = 0.1.

where $s \in [0, 1)$, when the control parameter $p \in (0, 0.5)$, the PWLCM system evolves into chaotic state [32]. The PWLCM system has uniform invariant distribution and very good ergodicity, confusion, and determinacy [33], so it can provide excellent random sequence, and the generated sequence is used to scramble the pixel position globally, which improves the security of the whole cryptosystem. The phase diagram of the PWLCM system with $p = 0.1$ is depicted in Figure 4. One-dimensional discrete chaotic system has the advantages of simple form and short time to generate chaotic sequence, but its disadvantage is that the key space is too small. Hyperchaotic system has more complex dynamic behavior, and it has stronger anti-interference ability and anti-deciphering ability. However, since the hyperchaotic system is more complex than the low-dimensional one, the time increase of the hyperchaotic sequence may directly affect the real-time requirement of secure communication. In the process of image encryption, the hyperchaotic system is used to increase the key space.

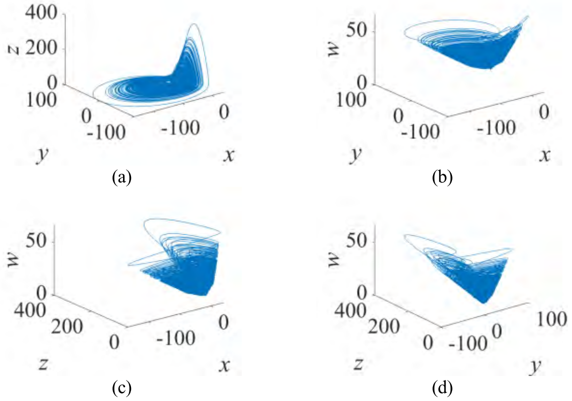
2) HYPERCHAOTIC ROSSLER SYSTEM

The Hyperchaotic Rossler system is a nonlinear dynamic system. It has the characteristics of an unpredictable motion trajectory, sensitivity to the control parameters and initial values, and boundedness of the motion trajectory. These characteristics are consistent with the cryptography research, and so the system is widely used in image encryption. The equation that describes a hyperchaotic Rossler system is shown in formula (2).

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay + w \\ \dot{z} = b + zx \\ \dot{w} = cw - dz, \end{cases} \tag{2}$$

where x, y, z, and w are the state variables, and a, b, c, and d are the control parameters. When $a = 0.25$, $b = 3$, $c = 0.05$, and $d = 0.5$, the above system is in a hyperchaotic state. The phase diagrams of the four planes, x-y-z, x-y-w, x-z-w, and y-z-w are shown in Figure 5.

III. ENCRYPTION ALGORITHM



(a) (b) (c) (d)

FIGURE 5. Phase diagrams of the different planes of a hyperchaotic Rossler system.

The hyperchaotic system is used to permute and scramble the pixels, the Hilbert curve is used to scramble the pixels, and the H-fractal structure is used to diffuse the pixels. Finally, the ciphertext feedback further enhances the confusion and diffusion abilities of the pixels, thus achieving image encryption.

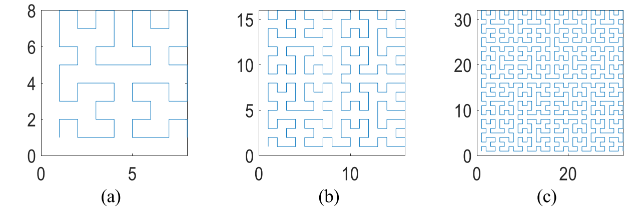
A. GENERATION OF CHAOTIC INITIAL VALUES

The Secure Hash Algorithm 3 (SHA-3) is one of the hash functions [34] that can convert arbitrarily long character information into hash values of the same length. The key that is generated by the hash value of the SHA-3 algorithm, even if the original image has a 1-bit difference, will be completely different, thus corresponding to a different encryption key. By associating the original image information with a hash function, it can generate a larger key space that will enhance the ability to resist exhaustive attacks, and the small changes in the plaintext can spread to the whole ciphertext image, which can be widely used in image encryption. Here we use the hash function to generate the key that is the initial value of the chaotic system in order to establish the association between the key and the plaintext image.

The original image is subjected to an SHA-3(256) operation to generate a set of 256-bit hash values, which are converted to binary values and used as the key K for the initial value of the chaotic system. The initial values generated by this method have the advantages of randomness and periodicity. The k is divided by bytes and can be divided into 32 bytes, expressed as $k_1, k_2, \ldots, k_{32}$. This will make $Q_1 = k_1 \oplus k_2 \oplus \ldots \oplus k_8$, $Q_2 = k_9 \oplus k_{10} \oplus \ldots \oplus k_{16}$, $Q_3 = k_{17} \oplus k_{18} \oplus \ldots \oplus k_{24}$, and $Q_4 = k_{25} \oplus k_{26} \oplus \ldots \oplus k_{32}$. The initial values of the hyperchaotic Rossler system and the PWLCM system are calculated as shown in formula (3).

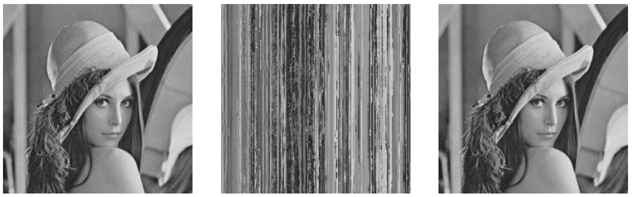
$$\begin{cases} x_0 = Q_1/256 + x'_0 \\ y_0 = Q_2/256 + y'_0 \\ z_0 = Q_3/256 + z'_0 \\ w_0 = Q_4/256 + w'_0 \\ S_0 = Q_4/256 + s'_0, \end{cases} \tag{3}$$

where x'_0, y'_0, z'_0, w'_0, and s'_0 are the given initial values.



(a) (b) (c)

FIGURE 6. **Three types of Hilbert scanning curves, (a) 8 × 8-order Hilbert curve, (b) 16 × 16-order Hilbert curve, (c) 32 × 32-order Hilbert curve.**



(a) (b) (c)

FIGURE 7. **The images after Hilbert scrambling, (a) plaintext Lena image, (b) a scrambled image, (c) decrypted Lena image.**

B. PIXEL SCRAMBLING

1) LOCAL SCRAMBLING

To scramble the image pixels locally by using the Hilbert curve, the pixel matrix of a given image is divided into four sub-matrices and scanned using the Hilbert curve. Then, the four sub-matrices are divided into four smaller sub-matrices and scanned using the Hilbert curve. By analogy, until each sub-matrix is a 2 × 2 pixel block, the Hilbert curve is scanned according to the Hilbert curve. The traversing path of the curve stores the pixel value of the image matrix A into another image matrix B at one time. The new image matrix B is the pixel matrix after traversing the Hilbert curve.

Three types of Hilbert scanning curves are illustrated in Figure 6, in which Figures 6(a)-(c) are an 8×8-order scanning curve, a 16×16-order scanning curve, and a 32×32-order scanning curve, respectively. Given a 256 × 256 Lena image, the Lena image that is scanned by the Hilbert curve is shown in Figure 7(b). By observation, it can be found that the original image has completely lost its features, which achieves the purpose of scrambling the plaintext image. After Hilbert scrambling, a Lena image is decrypted using the reverse operation of the Hilbert curve, and the image is shown in Figure 7(c). Therefore, using the Hilbert curve scan to scramble a plaintext image has a large number of scrambling paths and a great scrambling cycle and scrambling effect, which enhances the security of the image transmission.

2) GLOBAL SCRAMBLING

The Hilbert curve is suitable for local scrambling. Here we use the PWLCM system to achieve global scrambling. We iterate the PWLCM system $M \times N$ times and generate the chaotic sequences. The generated chaotic sequences are arranged in ascending order, and the permutation index sequence of each element in the sorted sequence in the original chaotic sequence is recorded. Then, the permutation matrix is filled according to each row of M values to obtain a permutation matrix, and the image's pixel positions are globally scrambled.

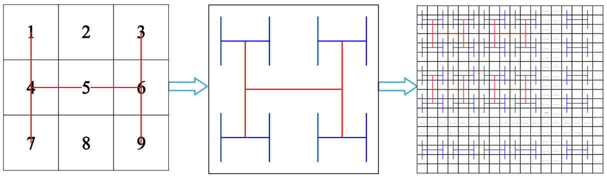
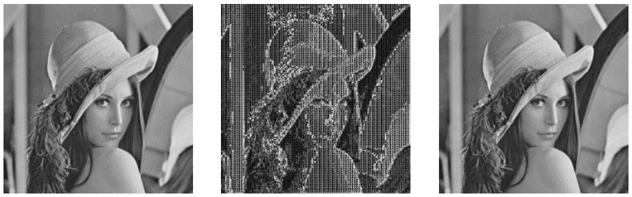


FIGURE 8. **The formation process of an H-fractal.**



(a) (b) (c)

FIGURE 9. **The image after H-fractal operations, (a) Plaintext Lena image, (b) The diffused image, (c) Decrypted Lena image.**

C. PIXEL DIFFUSION

Diffusion technology is a technique to replace the image pixel values, and the change in a pixel value will affect the change in the other pixel values such that the pixels in the different positions are coupled. Then, the encrypted image can resist the known-plaintext attacks. Here, we use the H-fractal to conduct local diffusion of the image's pixel values. The formation process of a second-order H-geometric fractal is shown in Figure 8.

For a first-order H-fractal, the pixel values of endpoints 1 and 7 are bitwise exclusive OR operations and are assigned to endpoint 1. The pixel values of endpoints 3 and 9 are bitwise exclusive OR operations and are assigned to endpoint 3. The pixel values of the two intersections 4 and 6 are bitwise exclusive OR operations and are assigned to point 4. The analogous operations are repeated throughout the image, as shown in Figure 8. Figure 9(b) is the image that was obtained after the H-fractal diffusion operation of the Lena image, and Figure 9(c) is the image that was obtained after the diffusion image is decrypted using the H-fractal reverse operation. It can be seen that the original image has changed significantly and that the diffusion process is reversible, but some features of the original image can still be seen. Therefore, we alternately use the H-fractal twice for the image diffusion operation to enhance the diffusion ability of the cryptosystem.

D. CIPHERTEXT FEEDBACK

The ciphertext diffusion operation makes minor changes to the plaintext that are spread to the whole ciphertext, thereby disrupting the relationship between the plaintext image and the ciphertext image. It can effectively resist cryptographic

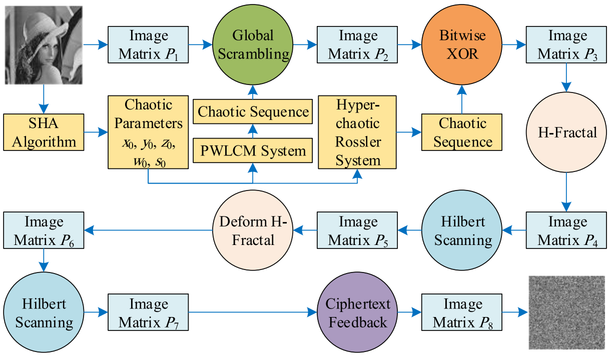


FIGURE 10. **Flowchart of the encryption process.**

attacks such as the chosen plaintext attacks and realize ciphertext diffusion. The image matrix is converted into a one-dimensional sequence $S = \{s_1, s_2, s_{3,} \ldots, s_{M\times N}\}$ of length $M \times N$ in the first order row. Then, let the sequence of the ciphertext diffusion be $SE = \{se_1, se_{2,}\ se_3, \ldots, se_{M\times N}\}$. The ciphertext diffusion is as follows in formula (4):

$$se(i) = s(i) \oplus se(i-1), \tag{4}$$

where the initialization elements are $se(0) = 128$, and $i = 1, 2, \ldots, M \times N$.

E. ENCRYPTION PROCESS

The digital image encryption algorithm proposed in this paper combines the Hilbert scanning curve and the H-geometric fractal structure, which mainly includes the following steps. First is position scrambling, which uses the chaotic sequences generated by the chaotic map to scramble and disturb the image pixels. Second, the Hilbert curve scanning and the H-geometric fractal were alternately used to realize the scrambling of the pixel positions and the diffusion of the pixel values. Finally, the pixel is further diffused through the ciphertext feedback. The encryption flowchart is shown in Figure 10, and the specific steps are as follows.

Step1: Convert the grayscale image P into a two-dimensional image matrix P_1 of size $M \times N$.

Step2: The SHA-3 hash function is used to calculate the hash value K of the image matrix P_1, and the chaotic initialization parameters x_0, y_0, z_0, w_0, and s_0 are obtained.

Step3: Use the one-dimensional PWLCM system to generate chaotic sequences and conduct global scrambling of the image matrix P_1, and the image matrix P_2 is obtained.

Step4: Iterate the hyperchaotic Rossler system to generate four chaotic sequences with lengths of $M \times N/4$. Then, take the third to thirteenth digits after the decimal point and conduct 256 modular operations on them. The $M \times N$ sequence matrix is composed of N elements in each row, and the sequence matrix and image matrix P_2 are subjected to a bitwise OR operation to obtain the diffused image matrix P_3.

Step5: The image matrix P_4 is obtained by using the H-geometric fractal for the first diffusion operation of the image matrix P_3.

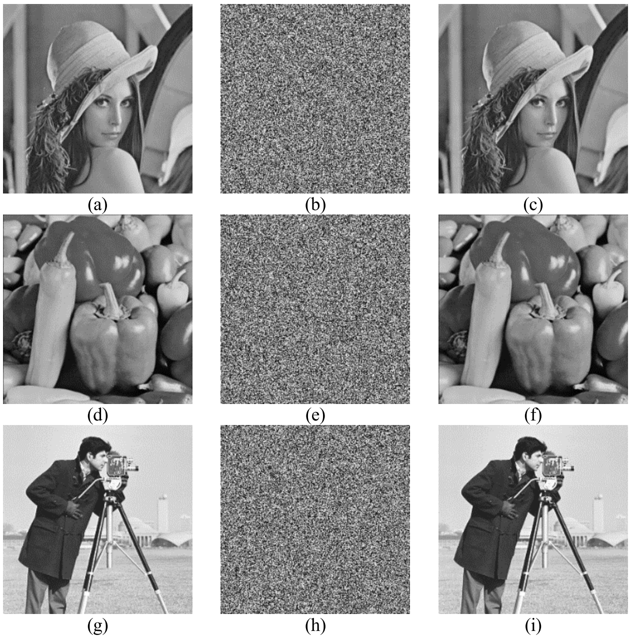


FIGURE 11. **Experimental results of the proposed technique. (a) Lena image. (b) Lena cipher image. (c) Lena decrypted image. (d) Peppers image. (e) Peppers cipher image. (f) Peppers decrypted Image. (g) Cameraman image. (h) Cameraman cipher image. (i) Cameraman decrypted image.**

Step6: The image matrix P_5 is obtained by using the Hilbert scanning curve in the image matrix P_4.

Step7: The second-order H-geometric fractal that is formed by the iteration of Step 5 is rotated clockwise by 90 degrees to obtain the deformed H-geometric fractal. The H-geometric fractal that deforms the image matrix P_5 is also used for the image diffusion operation to obtain the image matrix P_6.

Step8: The image matrix P_7 is obtained from the final round of the Hilbert scanning operation of the image matrix P_6.

Step9: The ciphertext feedback operation is performed on the scanned image of the Hilbert curve to obtain the matrix P_8, namely, the ciphertext image.

The decryption algorithm is the inverse of the above process, and the algorithm is also applicable to color image encryption, which only needs RGB decomposition of the image's pixel values.

IV. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

In this paper, the standard Lena, Peppers, and Cameraman gray images of size 256 × 256 are used to verify the feasibility and effectiveness of the algorithm. The algorithm is simulated using MATLAB 2018a on the Windows 10 operating system. The initial parameters $x'_0 = -50, y'_0 = -15$, $z'_0 = 70, w'_0 = 35$, and $s'_0 = 0$ are obtained by using the Gram-Schmidt standard orthogonalization method and the fourth-order Runge-Kutta algorithm. The plaintext, ciphertext and decrypted images of Lena, Peppers, and Cameraman are shown in Figure 11, respectively.

A good encryption algorithm should have enough key space to resist exhaustive attacks. The algorithm is sensitive

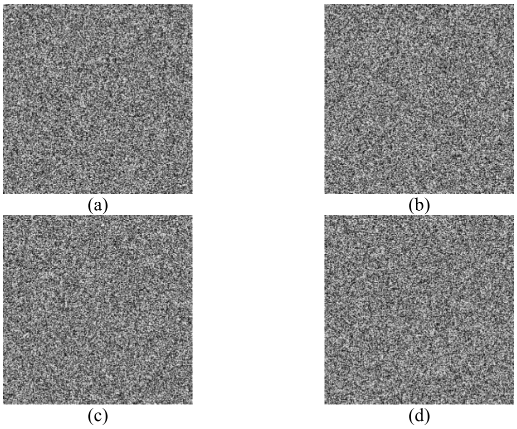


FIGURE 12. Decryption diagrams after small changes in the keys. (a) Decryption diagram of the $x_0 + 10^{-8}$ key. (b) Decryption diagram of the key $y_0 + 10^{-8}$ key. (c) Decryption diagram of the key $z_0 + 10^{-8}$ key. (d) Decryption diagram of the key $w_0 + 10^{-8}$ key.

to keys and can resist common attacks, such as statistical attacks, differential attacks, data loss attacks, noise attacks, and cropping attacks. This part mainly analyzes and discusses the performance and security of the proposed encryption method.

A. EXHAUSTIVE ATTACK ANALYSIS

1) KEY SPACE ANALYSIS

The encryption keys in this paper include x_0, y_0, z_0, w_0, l_0, and the 256-bit hash values. For the initial values x_0, y_0, z_0, and w_0 of the hyperchaotic Rossler system and the initial value s_0 of the PWLCM system, if the calculation accuracy is 10^{-8}, the key space size is 10^{40}, and the key space of the 256-bit hash values is 2^{128}, which means that the total key space of the encryption system is $S = 10^{40} \times 2^{128} = 3.40 \times 10^{78}$. Therefore, there is a large enough key space to resist exhaustive attacks.

2) KEY SENSITIVITY ANALYSIS

To test the sensitivity of the keys, for the hyperchaotic Rossler system, the initial values of x_0, y_0, z_0, and w_0 are increased by 10^{-8} and the other keys are unchanged. Figure 12 shows the corresponding decrypted image. The encryption keys x_0, y_0, z_0, and w_0 are changed 10^{-8}, respectively. The original keys and the modified keys are used to encrypt the three images, and the NPCRs and UACIs of the two cipher images are calculated, as shown in Table 1. The decryption keys x_0, y_0, z_0, and w_0 are changed 10^{-8}, respectively. The original keys and the modified keys are applied to decrypt the three images, and the NPCRs and UACIs of the two plain images are calculated, as shown in Table 2. It can be seen that the small changes in the keys cannot correctly decrypt the original image, and so the algorithm has strong key sensitivity.

B. STATISTICAL ATTACK ANALYSIS

1) HISTOGRAM ANALYSIS

To some extent, the statistical characteristics of the images can reflect the distribution of the gray values of the original images. Whether the statistical distribution of the original images can be changed is also an important evaluation index in image encryption [35], [36]. The purpose of this algorithm is to resist gray statistics attacks. The statistical histograms of the Lena, Peppers, and Cameraman plain images and the cipher images are shown in Figure 13. From the experimental results, it can be concluded that the statistical histograms of the encrypted images obtained by the pixel diffusion and replacement operations are very uniform, which shows that the algorithm has good resistance to statistical attacks, and the attacker cannot analyze the original gray value distribution range.

TABLE 1. Key sensitivity analysis in encryption process.

Metrics (%)		Lena	Peppers	Cameraman
x_0	NPCR	99.6231	99.6109	99.5651
	UACI	33.5321	33.4425	33.4992
y_0	NPCR	99.6246	99.6002	99.5926
	UACI	33.3530	33.4549	33.4689
z_0	NPCR	99.5865	99.6246	99.5911
	UACI	33.4180	33.4043	33.6870
w_0	NPCR	99.6017	99.5743	99.6262
	UACI	33.5293	33.4215	33.4932

TABLE 2. Key sensitivity analysis in decryption process.

Metrics (%)		Lena	Peppers	Cameraman
x_0	NPCR	99.4110	99.4370	99.4781
	UACI	27.6737	28.9922	32.6395
y_0	NPCR	99.4675	99.4431	99.3317
	UACI	25.6549	26.2443	30.2600
z_0	NPCR	91.4703	91.3666	91.4871
	UACI	25.5309	26.4983	28.2465
w_0	NPCR	99.0952	99.0112	99.1028
	UACI	26.6241	27.4034	32.2962

TABLE 3. Chi-square test results of plain images and cipher images.

Images	Plain image	Cipher image	P value	Decision
Lena	3.9851×10^4	260.4141	0.4823	Accept
Peppers	3.1630×10^4	254.7656	0.4807	Accept
Cameraman	1.6127×10^5	268.8047	0.4952	Accept

Chi-square test: Chi-square (χ^2) is an important criterion for analyzing uniformity of a histogram [37]–[40]. The calculation method is as follows:

$$\chi^2 = \sum_{i=1}^{256} \frac{(f_i - g)^2}{g}, \tag{5}$$

where g is the expected frequency and $g = (M \times N)/256$, M and N are the size of an image, and f_i is the observed frequency of a gray value i ($0 \leq i \leq 255$).

When the significant level is 0.05, and the corresponding ideal chi-square value is 293.2478. The results of the calculation are shown in Table 3. As can be seen from the results that the ciphertext chi-square values are less than 293.2478, and our encryption technique passed the chi-square test. Therefore, the proposed encryption technique in this paper can effectively resist statistical attacks.

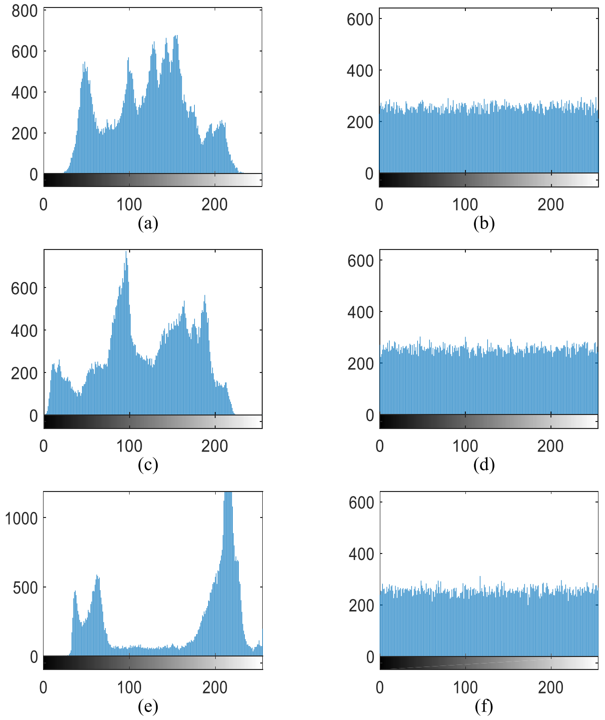


FIGURE 13. Histogram analysis of the three plain images and cipher images, (a) statistical histogram of the Lena plain image, (b) statistical histogram of the Lena cipher image, (c) statistical histogram of the Peppers plain image, (d) statistical histogram of the Peppers cipher image, (e) statistical histogram of the Cameraman plain image, (f) statistical histogram of the Cameraman cipher image.

2) CORRELATION ANALYSIS

The correlation of the adjacent pixels is an important evaluation index of digital image security analysis [41], [42], which reflects the scrambling degree of an image's pixel distribution. The smaller the correlation of the adjacent pixels in an encrypted image, the better is the scrambling effect, and vice versa, the worse is the scrambling effect. The correlation between the adjacent pixels of a plain image is very strong, and thus, attackers can easily obtain plaintext information by various means. The purpose of using an image encryption method is to reduce the correlation between the pixels and obtain the relevant cipher image. Taking the Lena image and its cipher image as an example, 10,000 pairs of adjacent pixels are randomly selected, and their correlation curves in the horizontal, vertical, positive, and negative directions are obtained as shown in Figure 14. According to formulas (6)-(9), the correlation coefficients in the horizontal, vertical, positive, and negative directions are calculated, respectively.

$$E\left(x\right)=\frac{1}{N}\sum\nolimits_{i=1}^{N}x_i, \qquad (6)$$

$$D\left(x\right)=\frac{1}{N}\sum\nolimits_{i=1}^{N}\left(x_i-E\left(x\right)\right)^2, \qquad (7)$$

$$cov\left(x,y\right)=\frac{1}{N}\sum\nolimits_{i=1}^{N}\left(x_i-E\left(x\right)\right)\left(y_i-E\left(y\right)\right), \qquad (8)$$

$$\rho_{xy}=\frac{cov\left(x,y\right)}{\sqrt{D\left(x\right)}\times\sqrt{D\left(y\right)}}, \qquad (9)$$

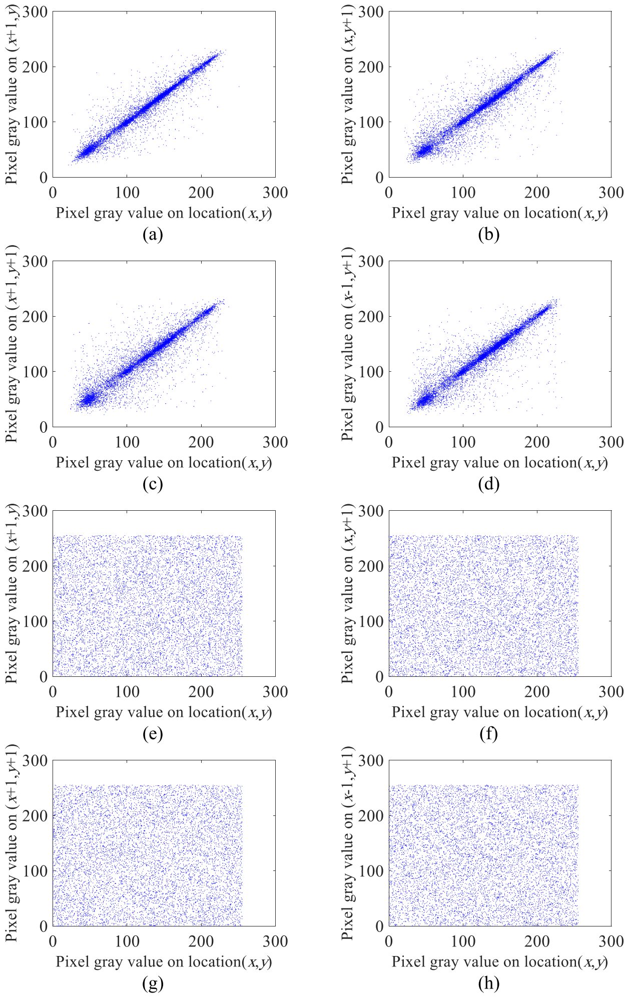


FIGURE 14. Correlation analysis of the Lena plain image and the Lena cipher image in four directions. (a) Horizontal correlation of the Lena plain image. (b) Vertical correlation of the Lena plain image. (c) Positive diagonal correlation of the Lena plain image. (d) Negative diagonal correlation of the Lena plain image. (e) Horizontal correlation of the Lena cipher image. (f) Vertical correlation of the Lena cipher image. (g) Positive diagonal correlation of the Lena cipher image. (h) Negative diagonal correlation of the Lena cipher image.

where x and y are the gray values of the adjacent pixels in the image, N represents the number of selected sample points, $E(x)$ is the mean, $D(x)$ is the variance, and $cov(x, y)$ is the covariance. Similarly, the correlation coefficients of the adjacent pixels between the plain image and the cipher image are shown in Table 4, which shows that the algorithm has good security.

3) INFORMATION ENTROPY ANALYSIS

Information entropy represents the degree of uncertainty of the system. It can be used to express the uncertainty of image information. The more confused the image information is, the higher the information entropy. For a gray image, the more uniform the distribution of the gray values is, the greater the information entropy, the greater the randomness, and the higher the security. The formula for the global Shannon

TABLE 4. The correlation coefficients of the plain and cipher images of the three groups of images in the horizontal, vertical, positive diagonal, and negative diagonal directions.

Images		Horizontal	Vertical	Positive diagonal	Negative diagonal
Lena	Plain image	0.9644	0.9332	0.9035	0.9236
	Cipher image	0.0015	-0.0014	-0.0028	-0.0037
Peppers	Plain image	0.9694	0.9651	0.9419	0.9434
	Cipher image	-0.0035	0.0050	0.0025	-0.0059
Cameraman	Plain image	0.9524	0.9194	0.8984	0.9031
	Cipher image	0.0072	-0.0113	-0.0065	-0.0040

TABLE 5. The results of information entropy.

Images	Plain image entropy	Global entropy	Local entropy	Result
Lena	7.4532	7.9979	7.9023	Passed
Peppers	7.5797	7.9976	7.9026	Passed
Cameraman	6.9046	7.9975	7.9021	Passed

entropy is defined as follows:

$$H\left(m\right) = -\sum\nolimits_{i=0}^{L} P\left(m_i\right) log_2 P\left(m_i\right), \tag{10}$$

where L is the gray level of the image, m_i is the i th gray value on the image, and $P\left(m_i\right)$ is the probability that m_i appears. For an $L = 256$ gray image, the theoretical value of the global entropy is 8. The closer the global entropy is to the theoretical value, the less likely the image will be attacked. Wu *et al.* proposed a calculation method named 'local Shannon entropy', which overcomes the shortcomings of inaccuracy, inconsistency, and low efficiency of global entropy [43], [44]. Local entropy is an improved method of global entropy. Local entropy randomly selects non-overlapping blocks in the image and then calculates the average value of the Shannon entropy. The (k, T_B)-local Shannon entropy on the image block is defined as follows:

$$\overline{H_{(k,T_B)}(S)} = \sum\nolimits_{i=1}^{k} \frac{H(S_i)}{k}, \tag{11}$$

where $S_1, S_2, \ldots, S_k$ are non-overlapping blocks with T_B pixels randomly chosen from encrypted image. $H(S_i)$ $(i = 1, 2, \ldots, k)$ represents the information entropy of S_i. We set $k = 30, T_B = 1936$ and randomly select k image blocks with T_B pixel for test. And the range of (30, 1936)-local Shannon entropy should be between [7.901901305, 7.903037329], with respect to α-level confidence of 0.05. Table 5 shows the results of the information entropy for multiple images. It can be seen from the results that the cipher image possesses high randomness.

C. DIFFERENTIAL ATTACK ANALYSIS

A differential attack makes small changes in the plain image and then encrypts the plain image and the changed image. The relationship between the plain image and the cipher image is obtained by comparing two encrypted images. Normally, two criteria, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI), are used to measure whether the encryption method can resist differential attacks. The mathematical formulas are as follows:

TABLE 6. Comparative analysis of the NPCRs and UACIs of the three groups of images.

Images	Lena	Peppers	Cameraman
NPCR (%)	99.5636	99.6292	99.6445
UACI (%)	33.4417	33.3796	33.6711

$$C\left(i,j\right) = \begin{cases} 0, & if\ P_1\left(i,j\right) = P_2\left(i,j\right) \\ 1, & if\ P_1\left(i,j\right) \neq P_2\left(i,j\right), \end{cases} \tag{12}$$

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\%, \tag{13}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} \left|P_1\left(i,j\right) - P_2\left(i,j\right)\right|}{255 \times M \times N} \times 100\%, \tag{14}$$

where M and N represent the length and width of the image, respectively, $P_1(i,j)$ and $P_2(i,j)$ represent the corresponding ciphertext pixel values before and after the plaintext changes, respectively. The closer the NPCR is to 100%, the more sensitive the image encryption scheme is to the plain image, and the stronger its ability to resist differential attack. The ideal values of NPCR and UACI are 99.6094% and 33.4635%, respectively. The closer the values are to their ideal values, the stronger is the method's ability to resist differential attacks. The NPCRs and UACIs of the three images and their comparisons with other references are shown in Table 6. As can be seen from the results that this scheme has strong resistance to differential attacks.

D. NOISE ATTACK ANALYSIS

The anti-noise attack ability of a cryptosystem is the standard for measuring the anti-interference ability of the system. The information will be disturbed by noise in the transmission process, which distorts the cipher image, and then the deciphered image will be affected to a certain extent. Common noises are salt and pepper noise, Gauss white noise, and Poisson noise. To analyze the anti-noise ability of the encryption algorithm, salt and pepper noise with different intensities is added to the cipher image and decrypted image. The cipher image with noise and the deciphered image with noise are shown in Figure 15.

The mean square error (MSE) is the cumulative square error between two images, which is used to measure the avalanche effect. And the peak signal-to-noise ratio (PSNR) is usually used to quantitatively analyze the similarity between the plain image and the deciphered image.

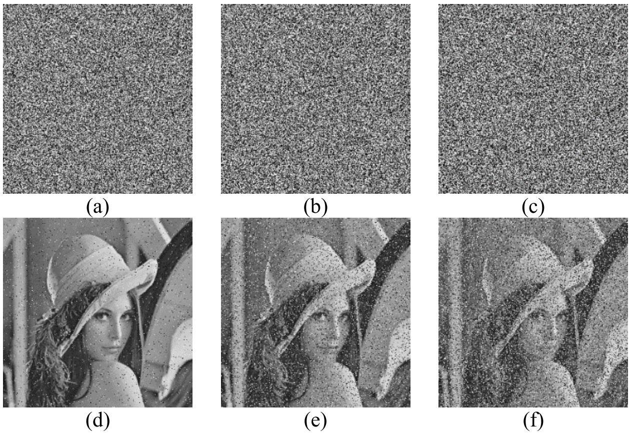


FIGURE 15. Cipher images with varying degrees of noise and corresponding decryption images. (a) Ciphertext with noise intensity of 0.01. (b) Ciphertext with noise intensity of 0.05. (c) Ciphertext with noise intensity of 0.1. (d) Decrypted image with noise intensity 0.01. (e) Decrypted image with noise intensity 0.05. (f) Decrypted image with noise intensity 0.1.

TABLE 7. The MSE, PSNR, and FSIM with the Lena images have varying degrees of noise added.

Noise intensities	MSE	PSNR	FSIM
0	0	∞	1
0.01	350.8314	22.6798	0.8853
0.05	1534.9511	16.2698	0.6349
0.1	2817.0228	13.6329	0.4937

The mathematical formulas of the MSE and PSNR are described as follows:

$$MSE = \frac{1}{M \times N} \sum\nolimits_{i=1}^{N} \sum\nolimits_{j=1}^{M} \left| C_1(i,j) - C_2(i,j) \right|^2, \quad (15)$$

$$PSNR = 20log_{10}\left(\frac{255}{\sqrt{MSE}}\right), \quad (16)$$

where M and N represent the height and width of the image, respectively, $C_1(i,j)$ and $C_2(i,j)$ represent the gray value of the plain image and the deciphered image at point (i,j), respectively.

The feature similarity index (FSIM) is the similarity score calculated using the FSIM algorithm, which is shown in literatures [45]–[47]. FSIM is used to measure the similarity between two images. When the FSIM between the two images is close to 1, there is a strong similarity between the two images. The MSE, PSNR, and FSIM between the plain image and the deciphered image are shown in Table 7. The correlations between the plain image and the deciphered image are shown in Table 8. Through comparative analysis, it can be seen that the encryption algorithm has a better anti-noise attack ability.

E. CROPPING ATTACK ANALYSIS

A good image encryption algorithm can still restore the plain image features after different degrees of cropping of the cipher image. The cipher image is cropped as shown in Figures 16(a)-(d), and then the restoration degree of the deciphered image relative to the plain image is analyzed. The cipher images are cut by 1/64, 1/16, 1/4, and 1/2, respectively, and then decrypted. The results are shown in Figures 16(e)-(h). The results of the correlations in four directions of the Lena deciphered images under different cropping intensities are shown in Table 9. The MSE, PSNR, and FSIM between the plain image and the deciphered image are shown in Table 10. It can be seen that when the cipher image is subjected to different degrees of cropping attacks, the plain image features can be restored to a certain extent. Therefore, the algorithm has a good ability to resist cropping attacks.

TABLE 8. Correlations in the four directions after the Lena images have varying degrees of noise added.

Noise intensities	Horizontal	Vertical	Positive diagonal	Negative diagonal
0	0.9644	0.9332	0.9035	0.9236
0.01	0.8314	0.7997	0.7817	0.7959
0.05	0.4807	0.4939	0.4568	0.4645
0.1	0.2601	0.2754	0.2711	0.2521

TABLE 9. Correlations in the four directions of the Lena deciphered images under different cropping intensities.

Cropping intensities	Horizontal	Vertical	Positive diagonal	Negative diagonal
1/64	0.8797	0.8575	0.8225	0.8521
1/16	0.7057	0.6661	0.6355	0.6480
1/4	0.2957	0.2830	0.2794	0.2896
1/2	0.0718	0.0721	0.0644	0.0699

TABLE 10. The MSE, PSNR, and FSIM with the Lena images have varying degrees of cropping added.

Cropping intensities	MSE	PSNR	FSIM
1/64	209.8402	24.9119	0.9316
1/16	745.0669	19.4089	0.7814
1/4	2541.2408	14.0803	0.5139
1/2	5046.4875	11.1009	0.3854

F. COMPUTATIONAL COMPLEXITY ANALYSIS

The time consumption part of any chaotic map based encryption algorithm is the generation of the chaotic sequences, scramble operations, and diffusion operations. This algorithm uses the PWLCM system and Rossler system based chaotic sequences, Hilbert scanning based scramble operations, and H-fractal and ciphertext feedback based diffusion operations. The proposed algorithm uses gray images of size $M \times N$ to perform encryption operations. M and N denote the row and column of the image.

In the chaotic sequence generation stage, the computational complexity of generating the PWLCM system and the Hyper-chaotic Rossler system are $O(M \times N)$. This increases the efficiency of the proposed algorithm as compared to the other image encryption method.

In the scramble stage, the Hilbert scanning based scramble operations are performed. Scrambling of pixel elements

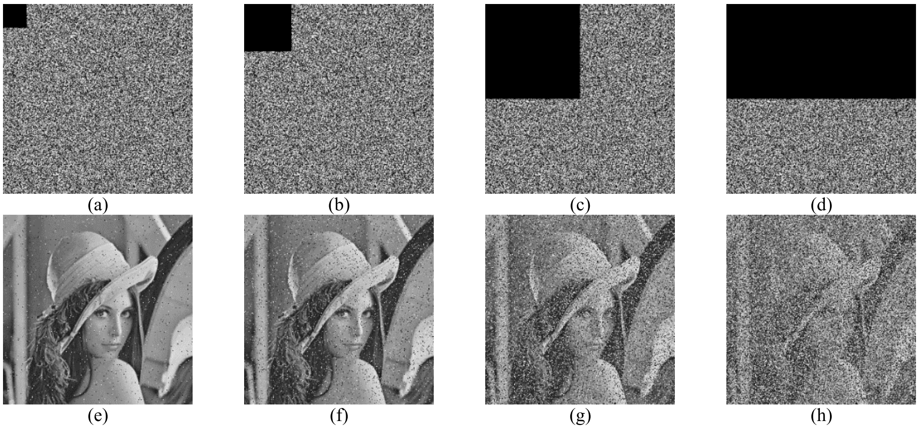


FIGURE 16. Deciphered Lena cipher images with different cropping Intensities. (a) Lena cipher image with 1/64 cropping. (b) Lena cipher image with 1/16 cropping. (c) Lena cipher image with 1/4 cropping. (d) Lena cipher image with 1/2 cropping. (e) Lena deciphered image with 1/64 cropping. (f) Lena deciphered image with 1/16 cropping. (g) Lena deciphered image with 1/4 cropping. (h) Lena deciphered image with 1/2 cropping.

TABLE 11. Comparisons of the encryption time between the proposed scheme and other literatures (seconds).

Images	Lena	Peppers	Cameraman
Ref [48]	0.53	0.60	0.67
Ref [49]	0.48	0.53	0.65
Ref [50]	0.57	0.66	0.72
Proposed	0.93	0.95	0.99

means shifting of pixel elements. The shift operations may be left or right and up or down. Hence the computational complexity of the two round of the Hilbert scanning is $O(2 \times M \times N)$. Therefore, the proposed algorithm is more efficient than other technique.

In the diffusion stage, the H-fractal and ciphertext feedback based diffusions are conducted. All the diffusion operations are performed by using bitwise XOR operations. the computational complexity of the two round of the H-fractal is $O(2 \times M \times N)$. Hence the overall computational complexity of the proposed cryptosystem is $O(5 \times M \times N)$.

G. SPEED ANALYSIS

To evaluate the running speed, tests are performed on the encryption speed of the proposed algorithm in comparison with other algorithms. The speed analysis is evaluated in a system that have configurations 3.5GHz processor with 8GB RAM and Windows 10 operation system. Table 11 shows the encryption time to encrypt different images using the proposed cryptosystem and the comparisons of encryption time between the proposed scheme and some existing image encryption schemes.

H. PERFORMANCE COMPARISON ANALYSIS

This section compares the performance of proposed scheme and other schemes for Lena image with the size 256 × 256. The comparison has done in terms of correlation coefficient, NPCR, UACI, and entropy and tabulated in Table 12. Simulation results and security analyses demonstrate that the proposed algorithm has large key space, high sensitivity to the keys and can resist well-known attacks, such as, statistical attack, differential attack, noise attack, and cropping attack. All these features illustrate that our algorithm is very suitable for image encryption and it can be applied in the secure communication of image files. Due to the use of a 4D hyperchaotic system, the computational complexity and simulation time computed by our algorithm is a little higher compared with some existing studies, and in the future, we will improve this encryption technique and design other algorithm to attain the combination of high security and quick speed.

TABLE 12. Performance comparisons with the existing methods for Lena image in size 256 × 256.

Metrics	Horizontal coefficient	Vertical coefficient	Diagnal coefficient	NPCR	UACI	Entropy
Padmapriya *et al.* [51]	-0.0033	0.0033	0.0117	99.62	33.45	7.9975
Chai *et al.* [52]	0.0114	-0.0011	-0.0032	66.61	33.46	7.9969
Ravichandran *et al.* [53]	-0.0025	-0.0016	0.0116	99.59	33.43	7.9972
Guo *et al.* [54]	-0.0074	0.0069	-0.0191	99.50	31.6551	7.9963
Bakhshandeh *et al.* [55]	-0.0063	0.0095	0.0089	99.46	37.6389	7.9974
Ye *et al.* [56]	0.0008	0.0016	0.0115	99.3011	34.5754	7.9970
Proposed	0.0015	-0.0014	-0.0028	99.5636	33.4417	7.9979

V. CONCLUSIONS

By combining the Hilbert scanning curve with the H-geometric fractal structure, a chaotic image encryption algorithm is proposed. Through Hilbert scanning, the H-geometric fractal and chaotic systems, two rounds of pixel position scrambling and pixel value diffusion are realized. The experimental results show that the algorithm has a large key space to resist exhaustive attacks and can also resist statistical attacks, differential attacks, noise attacks, and cropping attacks. It can be widely used in secure image information transmissions.

REFERENCES

[1] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons Fractals*, vol. 38, no. 1, pp. 213–220, Oct. 2008.

[2] W. M. Chen, C. J. Lai, H. C. Wang, H. C. Chao, and C. H. Lo, "H.264 video watermarking with secret image sharing," *IET Image Process.*, vol. 5, no. 4, pp. 349–354, Jun. 2011.

[3] 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.

[4] C. Zhu, C. Liao, and X. Deng, "Breaking and improving an image encryption scheme based on total shuffling scheme," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 25–34, Jan. 2013.

[5] 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.

[6] Y. Wang, C. Quan, and C. J. Tay, "Nonlinear multiple-image encryption based on mixture retrieval algorithm in Fresnel domain," *Opt. Commun.*, vol. 330, no. 1, pp. 91–98, Nov. 2014.

[7] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 38, pp. 5973–5978, Sep. 2008.

[8] Y. Zhang, D. Xiao, W. Wen, and M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlinear Dyn.*, vol. 76, no. 3, pp. 1645–1650, May 2014.

[9] H.-M. Yuan, Y. Liu, L.-H. Gong, and J. Wang, "A new image cryptosystem based on 2D hyper-chaotic system," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8087–8108, Mar. 2017.

[10] S. Dhall, S. K. Pal, and K. Sharma, "Cryptanalysis of image encryption scheme based on a new 1D chaotic system," *Signal Process.*, vol. 146, pp. 22–32, May 2018.

[11] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, pp. 749–761, Jul. 2004.

[12] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, nos. 1–3, pp. 153–157, 2005.

[13] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons, Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[14] A. Awad, "A new chaos-based cryptosystem for secure transmitted images," *IEEE Trans. Comput.*, to be published.

[15] A. A. A. El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 136–143, 2013.

[16] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dyn.*, vol. 75, no. 3, pp. 567–576, Feb. 2014.

[17] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, Dec. 2015.

[18] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Opt. Lasers Eng.*, vol. 80, pp. 1–11, May 2016.

[19] P. Ping, J. Wu, Y. F. Mao Xu, and J. Fan, "Design of image cipher using life-like cellular automata and chaotic map," *Signal Process.*, vol. 150, pp. 233–247, Sep. 2018.

[20] 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.

[21] M. A. Alia and A. B. Samsudin, "A new digital signature scheme based on Mandelbrot and Julia fractal sets," *Amer. J. Appl. Sci.*, vol. 4, no. 11, pp. 848–856, 2007.

[22] N. M. G. Al-Saidi and M. R. M. Said, "A new approach in cryptographic systems using fractal image coding," *J. Math. Statist.*, vol. 5, no. 3, pp. 183–189, 2009.

[23] S. Lian, X. I. Chen, and D. Ye, "Secure fractal image coding based on fractal parameter encryption," *Fractals*, vol. 17, no. 2, pp. 149–160, 2009.

[24] R. Anand, G. Bajpai, and V. Bhaskar, "Real-time symmetric cryptography using quaternion julia set," *Int. J. Comput. Sci. Netw. Secur.*, vol. 9, pp. 20–26, Mar. 2009.

[25] Y. Sun, L. Chen, R. Xu, and R. Kong, "An image encryption algorithm utilizing Julia sets and Hilbert curves," *PLoS ONE*, vol. 9, no. 1, Jan. 2014, Art. no. e84655.

[26] C.-H. Yuen and K.-W. Wong, "Cryptanalysis on secure fractal image coding based on fractal parameter encryption," *Fractals*, vol. 20, no. 1, pp. 41–51, Mar. 2012.

[27] S. I. Kamata, R. O. Eason, and Y. Bandou, "A new algorithm for N-dimensional Hilbert scanning," *IEEE Trans. Image Process.*, vol. 8, no. 7, pp. 964–973, Jul. 1999.

[28] X. Lin and L. Cai, "Scrambling research of digital image based on Hilbert curve," *Chin. J. Stereol. Image Anal.*, vol. 9, no. 4, pp. 224–227, Sep. 2004.

[29] K. Falconer, *Fractal Geometry: Mathematical Foundations and Applications*. Hoboken, NJ, USA: Wiley, 1990.

[30] K. A. K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-D chaotic maps," *J. Inf. Secur. Appl.*, vol. 46, pp. 23–41, Jun. 2019.

[31] X.-Y. Wang and L. Yang, "Design of pseudo-random bit generator based on chaotic maps," *Int. J. Mod. Phys. B*, vol. 26, no. 32, Dec. 2012, Art. no. 1250208.

[32] Y. Luo, R. Zhou, J. Liu, C. Yi, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.

[33] 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.

[34] X. Wang, S. Wang, Y. Zhang, and C. Luo, "A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems," *Opt. Lasers Eng.*, vol. 103, pp. 1–8, Apr. 2018.

[35] H. Diab, "An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations," *IEEE Access*, vol. 6, pp. 42227–42244, 2018.

[36] M. Li, D. Lu, W. Wen, H. Ren, and Y. Zhang, "Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata," *IEEE Access*, vol. 6, pp. 47102–47111, 2018.

[37] 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.

[38] X. Wang, Y. Hou, S. Wang, and R. Li, "A new image encryption algorithm based on CML and DNA sequence," *IEEE Access*, vol. 6, pp. 62272–62285, 2018.

[39] J.-M. Guo, D. Riyono, and H. Prasetyo, "Improved beta chaotic image encryption for multiple secret sharing," *IEEE Access*, vol. 6, pp. 46297–46321 , 2018.

[40] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A chaos based image encryption scheme using digit-level permutation and block diffusion," *IEEE Access*, vol. 6, pp. 67581–67593, 2018.

[41] 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, Aug. 2018, Art. no. 3901014.

[42] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.

[43] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 170–184, May 2016.

[44] 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.

[45] K. Gu, L. Li, H. Lu, X. Min, and W. Lin, "A fast reliable image quality predictor by fusing micro-and macro-structures," *IEEE Trans. Ind. Electron.*, vol. 64, no. 5, pp. 3903–3912, May 2017.

[46] K. Gu, G. Zhai, W. Lin, X. Yang, and W. Zhang, "No-reference image sharpness assessment in autoregressive parameter space," *IEEE Trans. Image Process.*, vol. 24, no. 10, pp. 3218–3231, Oct. 2015.

[47] L. Zhang, L. Zhang, X. Mou, and D. Zhang, "FSIM: A feature similarity index for image quality assessment," *IEEE Trans. Image Process.*, vol. 20, no. 8, pp. 2378–2386, Aug. 2011.

[48] 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.

[49] X. Chai, Z. Gan, and M. Zhang, "A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion," *Multimedia Tools Appl.*, vol. 76, no. 14, pp. 15561–15585, 2017.

[50] 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.

[51] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Medical data sheet in safe havens—A tri-layer cryptic solution," *Comput. Biol. Med.*, vol. 62, pp. 264–276, Jul. 2015.

[52] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019.

[53] D. Ravichandran, P. Praveenkumar, and J. B. B. Rayappan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017.

[54] Y. Guo, L.-P. Shao, and L. Yang, "Bit-level image encryption algorithm based on Josephus and Henon chaotic map," *Appl. Res. Comput.*, vol. 32, no. 4, pp. 1131–1137, Apr. 2015.

[55] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 665–673, 2013.

[56] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Opt. Commun.*, vol. 284, no. 22, pp. 5290–5298, Oct. 2011.

XUNCAI ZHANG was born in Zhoukou, China, in 1981. He received the Ph.D. degree from the Huazhong University of Science and Technology, in 2009. From 2010 to 2012, he accomplished the Postdoctoral Research at Peking University. He is currently an Associate Professor with the School of Electrical and Information Engineering, Zhengzhou University of Light Industry. His research interests include the areas of DNA computing and information security.

LINGFEI WANG received the bachelor's degree from Henan Polytechnic University, in 2016. He is currently pursuing the master's degree in electrical engineering with the Zhengzhou University of Light Industry. His research interests include the areas of DNA computing and information security.

ZHENG ZHOU received the bachelor's degree from Henan Agricultural University, in 2015. He is currently pursuing the master's degree in control theory and control engineering with the Zhengzhou University of Light Industry. His research interests include the areas of DNA computing and information security.

YING NIU received the master's degree from the Zhengzhou University of Light Industry, in 2009, where she is currently an Associate Professor with the School of Electrical and Information Engineering. Her research interests include the area of DNA computing and information security.