Research Article

An Image Encryption Algorithm Based on a New Hybrid Power Exponent Chaotic System

Dongyao Zou 1, Ming Li 1, Jun Li 2, and Zhigang Li 1

1Zhengzhou University of Light Industry, College of Computer and Communication Engineering, Zhengzhou 450000, China
2China Mobile Communications Group Henan Co. Ltd. Network Department, Zhengzhou 450000, China

Correspondence should be addressed to Dongyao Zou; zdy@zzuli.edu.cn

Received 29 August 2021; Revised 9 November 2021; Accepted 9 December 2021; Published 30 December 2021

Aiming at the problem of a small parameter value range when a one-dimensional chaotic system presents a chaotic state, this paper proposes a new type of hybrid power exponential chaotic system (HPECS). HPECS combines the classic one-dimensional Sine chaotic system to form a new chaotic system (HPECS-SS). Experiments show that the obtained new chaotic system has better chaotic performance, a more extensive parameter value range, and higher sensitivity. Simultaneously, on the basis of HPECS-SS, a new image encryption algorithm is proposed. The algorithm uses the key generated by the SHA-512 algorithm and HPECS-SS to iteratively output the chaotic sequence, SFY algorithm combines the chaotic sequence to perform two rounds of scrambling on the plaintext sequence to obtain the scrambling sequence, and finally, through the modulus operation to diffuse the scrambling sequence to form the encryption matrix of the plaintext image, simulation experiment analysis shows that the algorithm has a large key space, good encryption effect, and security; the pixel change rate (NPCR) and the normalized average change intensity (UACI) are close to ideal values which can resist various cryptanalysis and attacks.

1. Introduction

With the rapid development of the Internet and multimedia transmission technology, image information has become an essential part of people’s daily lives. Massive image information transmission makes image security become the focus of public attention. How to prove the security and confidentiality of image information has become a key research content in the field of information security [1]. Different from ordinary texts, digital images themselves have some unique characteristics, such as vivid images, intuitive expressions, etc., which enable images to be widely used; at the same time, digital images also have unique advantages such as a large amount of data and greater correlation between pixels, which are unmatched by ordinary text. Due to network transmission’s relatively high publicity, image transmission may encounter many security risks, such as copy, paste, tampering, etc. [2, 3]. And because the pixels between the images are relatively strong, if the general traditional encryption algorithm is used, it will cause the slow encryption speed, long encryption time, low efficiency, and other shortcomings, which are not enough to perform better encryption on the image. Therefore, encryption and decryption processing is required to ensure the secure transmission of images [4].

The chaotic system has the characteristics of pseudorandomness, extremely high sensitivity to initial values, and unpredictability, making it very suitable for image encryption systems and can improve the efficiency of the security of the encryption system [5–9]. In recent years, chaotic systems have also been extremely hot to be studied. Since the introduction of chaotic systems, there have been several research upsurges. The combination of chaotic system and image encryption has been well researched and used. The combination of the two can perform encryption well. Even if the encryption algorithm is public, a small change in the key will produce a completely different ciphered image, so many scholars have developed many excellent algorithms on this basis [10–12]. Image encryption includes two stages of scrambling and diffusion. Classical
replacement algorithms include Arnold-based replacement algorithm [13–15], Baker-based image replacement algorithm [16, 17], and cyclic shift replacement algorithm [18–21], and a permutation algorithm based on sorting. However, many chaotic sequences entangled by chaotic systems have such a problem. The initial conditions and parameters are randomly selected, which cannot resist image attacks very well. Therefore, a stream cipher algorithm based on a one-time key and robust chaotic mapping is designed in [22]. Piecewise linear chaotic mapping is used as the generator of the pseudorandom key stream sequence. The initial conditions are determined by the real random number generator. With generation, this algorithm makes even the same image; after encryption, it will be significantly different, ensuring the security level of the image. The image encryption algorithm studied in [23] uses a one-dimensional chaotic system and the hash value of each plane to rearrange the bit planes to achieve the effect of scrambling diffusion, which can effectively resist exhaustive attacks, statistical analysis attacks, and differential attacks.

In the previous image encryption, many researchers have improved a lot in the encryption algorithm scrambling and diffusion methods and have many good encryption effects, but they have done less innovation in chaotic mapping. One-dimensional chaotic systems are often used in encryption systems [24, 25], such as one-dimensional logistic systems, one-dimensional Sine systems, etc. Although one-dimensional systems have many advantages, many one-dimensional systems have shortcomings such as small key space, low confidentiality, slow encryption speed, and low efficiency [26–28]. At the same time, when a one-dimensional chaotic system presents a chaotic state, the parameter value range is relatively small, and the chaotic range is not uniform, so many researchers have modified it on the basis of the one-dimensional chaotic system to expand the value range of the chaotic system parameters. Tan et al. [29] mention the newly modified chaotic system IESL based on the exponential compound type. When the three parameters are within the range, LE is always greater than zero, which proves that the chaotic system modified in this article has strong robustness. If the chaotic map is improved to produce a more complex chaotic sequence, and then the image is encrypted, will there be a better encryption effect? In order to expand the value range of the parameters of the chaotic system and obtain a more complex chaotic sequence, so that the image encryption has better confidentiality, this paper proposes a new hybrid power exponential chaotic system (hybrid power exponential chaotic system: HPECS), which is substituted into a typical one-dimensional chaotic system to form a new chaotic system (HPECS-SS) compared with a typical one-dimensional chaotic system. Using bifurcation graph, Lyapunov exponent, Shannon entropy, etc., to analyse the chaotic performance of HPECS-SS, using the key generated by the SHA-512 algorithm and HPECS-SS to iteratively output the chaotic sequence, the SFY algorithm combined with the chaotic sequence performs two rounds of scrambling on the plaintext sequence to obtain the scrambling sequence, and finally the scrambling sequence is diffused to form the plaintext image through the modulo operation. In the encryption matrix, the simulation results prove that the encryption algorithm has better encryption performance.

The structure of this paper is as follows: Section 2 reviews the classic one-dimensional chaotic system and proposes HPECS and analyses HPECS-SS; Section 3 proposes an image encryption algorithm based on HPECS; Section 4 gives the decryption of the encryption algorithm scheme; Section 5 is the experimental analysis of the grayscale image encryption effect; Section 6 is the summary of this article.

2. The Proposed Chaotic System

2.1. Classical One-Dimensional Chaotic System. In the field of image encryption, commonly used chaotic systems include logistic chaotic system and Sine chaotic system. The logistic chaotic system is a classic one-dimensional chaotic system proposed by the mathematical ecologist Robert M. May. Due to the simple structure of the system and the good performance of chaotic behaviour, it has highly complex dynamic behaviour, so it is widely used in the field of information security [30]. The mathematical expression of the logistic chaotic system is

\[ x_{n+1} = \mu x_n (1 - x_n) (0 < x_n \leq 1) \]

where \( \mu \) is the system parameter, and \( x_n \) is the generated chaotic sequence. The bifurcation diagram of the logistic chaotic system is shown in Figure 1. The value range of parameter \( \mu \in (0, 4) \); when \( \mu \in (3.57, 4) \), the system exhibits chaotic behaviour, and the periodic window disappears, and when \( \mu = 4 \), the logistic mapping distribution presents the maximum state.

Sine chaotic system is also a commonly used one-dimensional chaotic system. The mathematical expression of the Sine chaotic system is

\[ x_{n+1} = M (\mu, x_n) = \mu \sin (\pi x_n) \]

The bifurcation diagram of the Sine chaotic system is shown in Figure 2. When \( \mu \in (3.478, 4) \), the system exhibits chaotic behaviour.

2.2. New Hybrid Power Exponent Chaotic System. The general mathematical expression of HPECS proposed in this paper is as follows:

\[ x_{n+1} = m (\mu + k (\mu, x_n)) \theta (\gamma, x_n) \]

where \( m \) is the system adjustment parameter, and its value will affect the system performance under the condition of fixed \( k (\mu, x_n) \), \( g (\gamma, x_n) \); \( k (\mu, x_n) \), \( g (\gamma, x_n) \) can be typical chaotic systems, such as logistic chaotic system and Sine chaotic system, etc. Based on the general mathematical expression of the HPECS system, this paper assigns the Sine chaotic system with the better chaotic performance to \( k (\mu, x_n) \), \( g (\gamma, x_n) \) to obtain a new chaotic system, HPECS-SS, whose mathematical expression is
For HPECS-SS, this paper makes a relevant analysis on the selection of $m$ parameters. For different values of $m$, the value range of the chaotic system is compared. It is found that the value range of HPECS-SS is relatively large when $m = 10$, and the variables that can make the system in chaotic behaviour can get better distributed in the phase space. In summary, the chaotic system expression used in the image encryption/decryption process in this paper is

$$x_{n+1} = \mu^{m} \left( \mu + \mu \frac{\sin (\pi x_n)}{4} \right)^{\mu \sin (\pi x_n)/4}.$$  \hspace{1cm} (4)

The system bifurcation diagram of HPECS-SS is shown in Figure 3. The value range of parameter $\mu \in (0, 6]$; when $\mu \in (1.402, 6)$, the system presents chaotic behaviour, and the bifurcation graph presents a chaotic state, and when $\mu \geq 1.402$, there is no periodic window.

In order to evaluate the characteristics of the chaotic mapping system of HPECS-SS proposed in this paper, in this section, the sensitivity of HPECS-SS, Shannon Entropy (SE), etc., will be discussed, and the one-dimensional logistic mapping and one-dimensional Sine mapping will be used to compare with HPECS-SS.

2.2.1. Sensitivity Analysis. The Lyapunov exponent (LE) is an important index to evaluate whether a nonlinear system has chaotic motion, and its mathematical expression is

$$LE = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|.$$  \hspace{1cm} (6)

The value LE of can be used to evaluate whether the chaotic map has reached the chaotic state at a certain moment. If LE $> 0$, the chaotic system is in a chaotic state. This paper uses the LE index to test the sensitivity of the chaotic system to the initial value. The test results of the logistic chaotic system, the Sine chaotic system, and the HPECS-SS chaotic system are shown in Figure 4.

It can be observed from Figure 4 that Logistic’s LE index shows that $\mu$ is greater than 0 after 3.57. When $\mu \geq 3.57$, the chaotic sequence obtained by the logistic chaotic system is not uniformly distributed in $[0, 1]$; the range where LE is greater than 0 is smaller, which will affect the security of the encryption scheme to a certain extent. The LE index of the Sine chaotic system is greater than 0 when $\mu \geq 3.478$; that is, a chaotic sequence is generated, which has the same problem as the chaotic series generated by logistic. The LE index value of HPECS-SS is greater than 0 after $\mu \geq 1.402$; that is, a chaotic sequence is generated. Therefore, it can be seen from the comparison that the usable value range of $\mu$ of HPECS-SS is larger than the other two one-dimensional chaotic maps.

2.2.2. Shannon Entropy Analysis. Shannon entropy is a nonlinear dynamic parameter that measures the incidence of information in a time series. It can be used to measure the complexity of the output sequence of the system, that is, the degree of irregularity. The larger the Shannon entropy value, the higher the complexity of the time series. This paper uses Shannon entropy to evaluate the complexity of the chaotic sequence generated by HPECS-SS. The Shannon entropy of logistic system, the Sine system, and HPECS-SS in this paper are shown in Figure 5. It can be seen from the figure that the
Figure 4: LE index diagram of three chaotic systems. (a) Logistic chaotic system; (b) sine chaotic system; (c) HPECS-SS chaotic system.

Figure 5: Shannon entropy of three chaotic systems.
Security and Communication Networks

Shannon entropy of HPECS-SS reaches its maximum at around 1.5, while the one-dimensional logistic chaotic system reaches its maximum at approximately 4, and the one-dimensional Sine system reaches its maximum at approximately 1.2 and then slowly decreases. It can be seen intuitively that the maximum SE of HPECS-SS is larger than the other two one-dimensional chaotic systems and almost reaches the ideal value. Therefore, the complexity of the output sequence of the new chaotic system is greater than that of the classic one-dimensional chaotic system.

3. Image Encryption Algorithm Based on HPECS-SS

The encryption algorithm proposed in this paper is based on HPECS-SS. The encryption process is divided into three stages: key generation, scrambling, and diffusion. The algorithm framework is shown in Figure 6.

3.1. Key Generation. Key $K = (x_0, \mu_0, x_1, \mu_1, x_2, \mu_2, N_0, \theta, L)$ has a total of 9 parameters, of which $x_0, x_1, x_2$ are the initial value, $\mu_0, \mu_1, \mu_2$ are the control parameter, $N_0$ is the iteration parameter, $\theta$ control the interception position of the hash sequence, and $L$ control the interception length of the hash sequence. The role of the key $K$ in the system is manifested in two aspects: (1) It is used to generate the initial value and control parameters of the chaotic system; (2) it is used to obtain the subkey in the scrambling-diffusion process.

First, discuss the key generation method in this article. The key generation depends on the SHA-512 algorithm. The hash function has the properties of irreversibility and collision resistance. Using these two properties in image encryption can effectively resist attacks on plaintext and ciphered. In order to achieve “one image, one key,” it is ensured that the key and the plaintext image have a strong correlation. According to equations (7) and (8), the plaintext information is used as the input of the SHA-512 algorithm, and a 512-bit hash value $\text{Hash}$ is obtained.

$$\text{Hash} = [\text{SHA} - 512(\text{P}_{\text{sum}})]_2. \quad (7)$$

$$\text{P}_{\text{sum}} = \sum_{i=1}^{M} \sum_{j=1}^{N} \text{P}(i, j), \quad (8)$$

where $\text{Hash}$ is a 512-bit binary number; $\text{P}_{\text{sum}}$ is the sum of all pixels of the plaintext image (image size is $M \times N$).

This article makes the following provisions:

$$H(\alpha, \beta) = \text{Hash}(\alpha: \beta) = \{h_\alpha, h_{\alpha+1}, \ldots, h_\beta\}, 1 \leq \alpha \leq \beta \leq 512. \quad (9)$$

In equation (10), $H(\alpha, \beta)$ represents a hash sequence of length $\beta - \alpha + 1$, $h_\alpha$ is the $\alpha$-th position of Hash, and $h_\alpha \in \{0, 1\}$.

In order to make the randomness of the initial value and control parameter generation of the chaotic system and the correlation with the plaintext image, a continuous sequence $H(\theta, \theta + L)H(\theta, \theta + L)$ of length $L$ is randomly selected from Hash, where $L \geq 8$ and $\theta$ are random integers and $\theta \in [0, 512 - L]$. $H(\theta, \theta + L)$ is used to generate the initial value $x_0$ and the control parameter $\mu_0$ that transform the plaintext image sequence into the chaotic image sequence, $x_0$ and $\mu_0$ should meet the conditions of equation (5), and the specific calculation equations are as equations (10)–(13).

$$\lambda_h = \frac{\text{XOR}(H(\theta, \theta + L))}{2^L}. \quad (10)$$

$$\lambda_p = \frac{P_{\text{sum}}}{M \times N} - \left[\frac{P_{\text{sum}}}{M \times N}\right]. \quad (11)$$

$$x_0 = \text{mod}(\lambda_h + \lambda_p, 1). \quad (12)$$

$$\mu_0 = \text{mod}(x_0, b_0) + c_0, \quad (13)$$

where XOR is the exclusive OR function. $\lambda_h$ guarantees the randomness generated by $x_0$ and $\mu_0$, and $\lambda_p$ guarantees the correlation between $x_0$ and $\mu_0$ and the plaintext image. In order to make $x_0$ and $\mu_0$ in a reasonable interval and avoid local chaotic behaviour, let $b_0 > 0$, $c_0 > 0$ here. Similarly, by controlling the values of $L$ and $\theta$, the initial values $x_1$ and $x_2$ and the control parameters $\mu_1$ and $\mu_2$ can be obtained.

For the generation of chaotic sequence, this paper substitutes $x_0$ and $\mu_0$ into equation (5) and iterates $M \times N + N_0$ times to generate a one-dimensional chaotic sequence of length $M \times N$. $N_0$ is used to eliminate the transient effect produced by the iterative process and the influence on the generation of the chaotic sequence.

3.2. Scrambling Stage. The sorting in this paper uses the Gonard scrambling algorithm (Sort Fisher-Yates: SFY), combining the sort scrambling algorithm and the Gonard scrambling algorithm (Fisher-Yates scrambling algorithm), to perform two rounds of sorting on the plaintext sequence. The Fisher-Yates scrambling algorithm is unbiased, and there are $n!$ equal probability arrangements for the sequence of length $n$.

The scrambling is divided into two rounds: one round of scrambling is to sort the plaintext sequence through the chaotic sequence to obtain a round of scrambling sequence $P' = \{p_1', p_2', \ldots, p_{M \times N}'\}$; the second round of scrambling is to scramble the sequence $S = \{s_1, s_2, \ldots, s_{M \times N}\}$ through the Fisher-Yates scrambling algorithm to obtain the scrambling sequence. The specific implementation steps are as follows:

Step 1: Substitute $x_0$ and $\mu_0$ into equation (5) to get the chaotic sequence $K^0 = \{k_1^0, k_2^0, \ldots, k_{M \times N}^0\}$ after $M \times N + N_0$ iteration.

Step 2: Sort the elements in the chaotic sequence $K^0$ in ascending order to obtain the position sequence $K' = \{k_1', k_2', \ldots, k_{M \times N}'\}$; obtain a round of scrambling sequence $P' = \{p_1', p_2', \ldots, p_{M \times N}'\}$ by the following equation:

$$p_i' = p_{k_i}. \quad (14)$$
3.3. Diffusion Stage. The diffusion process will modify the pixel value through a certain regular method to supplement the problem of only changing the position of the pixel during the scrambling process, which makes it difficult to effectively resist the problem of statistical attacks. The specific steps of the diffusion process in this paper are as follows:

Step 1: Substitute \( x_2 \) and \( \mu_2 \) into equation (5) to get the chaotic sequence \( K^2 = \{ k_1^2, k_2^2, \ldots, k_{M\times N}^2 \} \) after iteration.

Step 2: Incorporating \( K^2 = \{ k_1^2, k_2^2, \ldots, k_{M\times N}^2 \} \) and \( S = \{ s_1, s_2, \ldots, s_{M\times N} \} \) into equation (18), the correlation between the plaintext pixels in the scrambled sequence is diffused into the entire diffused chaotic sequence, and the diffused sequence \( Q = \{ q_1, q_2, \ldots, q_{M\times N} \} \) is obtained.

\[
q_i = \begin{cases} 
\text{mod}(S_{\oplus}(\left[ K_i^2 \times 2^F \right]), 2^F) \oplus \eta & i = 1 \\
\text{mod}(S_{\oplus}(\left[ K_i^2 \times 2^F \right]), 2^F) \oplus q_{i-1} & \text{other} 
\end{cases}
\]

where \( F \) is the pixel bit depth, and \( \eta \) is the control parameter in the diffusion process.

Step 3: Reshape the diffusion sequence \( Q \) into a matrix of \( M \times N \) to obtain the final encryption matrix \( Q \).

The pseudocode of the diffusion phase is shown below:

4. Decryption Process

The decryption process is the inverse process of the encryption process. For the image encryption algorithm proposed in this article, it should be noted in the decryption that equation (18) in the expansion process should be equation (19):

\[
S_i = \begin{cases} 
q_i \oplus q_{i-1} \oplus \text{mod}(S_{\oplus}(\left[ K_i^2 \times 2^F \right]), 2^F) & i = 1 \\
q_i \oplus Q_{i-1} \oplus \text{mod}(S_{\oplus}(\left[ K_i^2 \times 2^F \right]), 2^F) & \text{other} 
\end{cases}
\]

5. Simulation Results and Performance Analysis

5.1. Simulation Results. In this paper, the grayscale plaintext images of Lena, Peppers, and Cameraman with an image size of 256×256 are selected for simulation, and the simulation results are shown in Figure 7. The plaintext image, ciphered image, and decrypted image of the above three images are, respectively, given, where the information of the plaintext image still remains in the decrypted image.

5.2. Key Analysis

5.2.1. Key Space Analysis. Key space is the range of encryption key size, usually in bits. In order to resist brute force attacks, the encryption algorithm needs to have a large enough key space. In this article, the initial value of the chaotic system and the control parameters \( (x_0, \mu_0) \), \( (x_1, \mu_1) \), \( (x_2, \mu_2) \) and the hash sequence obtained through the plaintext image are the keys of the encryption algorithm. The space size of the hash sequence obtained by the SHA-512 algorithm is 2512. When the key space is greater than 2100, it is sufficient to resist brute force attacks [28]. The overall key space of this article is greater than 2512, which has a good effect on resisting brute force attacks.

5.2.2. Key Sensitivity Analysis. In order to verify that the key obtained by the algorithm in this paper has strong sensitivity, we set the parameters of \( x_0 \) to 3.838 and 3.826, respectively, and the ciphered images obtained are shown in
Figures 8(b) and 8(c). Although there is only a slight change in $x_0$, the obtained key difference is as high as 99.8784%; secondly, perform algebraic operations on the obtained $x_0 = 3.838$ to get $K^0 - 1$. The corresponding ciphered image is shown in Figure 8(d). The key difference between $K^0$ and $K^0 - 1$ reaches 99.9213%. The above results show that the encryption algorithm proposed in this paper is key-sensitive.

5.2.3. Key Randomness Analysis. This paper uses the NIST sequence randomness test tool to analyse the randomness of the generated key sequence. The test items include 15 items such as frequency test, intrablock frequency test, and linear complexity test. The values obtained for 15 test items are all greater than the significance level of 0.01. The results show that the generated key sequence has strong randomness.

5.3. Histogram Analysis. The histogram is used to describe the distribution of image pixel values. If the histogram is unevenly distributed, the attacker can obtain certain information through statistical analysis to crack our encryption scheme and analyse the characteristics of the ciphered image to make the ciphered attack easier. Therefore, in order to verify the maturity of the encryption scheme proposed in this article, the analysis of the histogram is necessary.

In this article, three pictures of Lena, Peppers, and Cameraman’s histogram distribution are given, as shown in Figure 9. It can be seen from the figure that the histogram distribution of the plaintext image is very uneven, while the distribution of the ciphered image is relatively uniform, and the average is near a certain value, indicating that the algorithm can resist statistical attacks well.
The smaller the variance value of the histogram, the higher the uniformity of the encrypted image, calculated by formula (20):

\[
\text{var} = \frac{1}{n^2} \sum_{i=0}^{n} \sum_{j=1}^{n} \frac{1}{2} (z_i - z_j)^2, \tag{20}
\]

where \(z_i\) and \(z_j\) are the number of pixels with gray values \(i\) and \(j\), respectively, \(n = M \times N\).

In the simulation experiment, we calculated the variance of the histogram of the three ciphered images of Lena, Peppers, and Cameraman by formula (20), and the calculation results are shown in Table 1. The variances of the three ciphered images of Lena, Peppers, and Cameraman are 5156.719, 5289.979, and 5154.814, respectively. In [15] and [31], the variances of Lena’s encrypted image histogram are 5554.829 and 5335.830, respectively, which are greater than any variance in Table 1. It shows that, in the histogram analysis, the algorithm we proposed is also effective.

In addition to visually analysing the difference between the plaintext image and the ciphered image from the histogram, this paper uses \(\chi^2\) detection to digitally detect whether the ciphered pixels are evenly distributed. The mathematical expression of the \(\chi^2\) distribution is

\[
\chi^2 = \sum_{i=0}^{n} \frac{(y_i - \bar{y})^2}{\bar{y}}, \tag{21}
\]
Figure 8: Key sensitivity analysis diagram. (a) Lena plaintext image; (b) Lena ciphered image \( (x_0 = 3.838, K_0) \); (c) Lena plaintext image \( (x_0 = 3.826, K_0) \); (d) Lena ciphered image \( (x_0 = 3.838 K_0 - 1) \).

Figure 9: Image histogram. (a) Lena Plaintext image; (b) Lena Ciphered image (c) Peppers Plaintext image; (d) Peppers Ciphered image; (e) Cameraman Plaintext image; (f) Cameraman Ciphered image.
where \( n \) is the gray level, and \( n \) is 255 in this paper; \( y_i \) is the frequency of pixel \( i \) in the image. Suppose the image size is \( M \times N \); there are

\[
\bar{K} = \frac{M \times N}{n + 1}
\]

When the confidence level is 0.05, \( \chi^2_{0.05} (255) = 293.24783 \); that is, when the \( \chi^2 \) detection value of the image is less than 293.24783, it passes the test. Table 2 shows the histogram \( \chi^2 \) test results of the plaintext image and ciphered image of Lena, Peppers, and Cameraman. The \( \chi^2 \) test results of the ciphered images of the three images are all less than 293.24783, so it can be judged that the ciphered image encrypted by this algorithm is closer to a uniform distribution.

5.4 Adjacent Pixels Correlation Analysis. The adjacent pixels of the image are generally closely related, and their distribution is in the diagonal direction. Because the image is scrambled and diffused by the encryption algorithm, the correlation of the pixels of the ciphered image will become relatively low, and the plaintext image can be obtained by resisting the destruction attack. In order to measure the correlation between the image before and after encryption in different directions (horizontal, vertical, and diagonal), this paper uses equation (22) to calculate the correlation coefficient. Take Lena as an example to test the correlation between the pixels of the plaintext image and the ciphered image. Figures 10 and 11 show the correlation distribution of Lena’s plaintext image and ciphered image in various directions, respectively. Figures 12 and 13 show the correlation distribution of Peppers’ plaintext image and ciphered image in various directions, respectively. Figures 14 and 15 show the correlation distribution of Cameraman’s plaintext image and ciphered image in various directions, respectively.

\[
r_{mn} = \frac{\text{cov}(m, n)}{\sqrt{D(m)} \sqrt{D(n)}}
\]

\[
\text{cov}(m, n) = E[(n - E(n))(m - E(m))]
\]

\[
E(m) = \frac{1}{N} \sum_{i=1}^{N} m_i, D(m) = \frac{1}{N} \sum_{i=1}^{N} (m_i - E(m))^2
\]

5.5 Information Entropy. In image encryption, information entropy can measure the distribution of information sources. For a grayscale image with a grayscale level of 256, the theoretical value of information entropy is 8. That is, the closer the value of the ciphered image information entropy of the grayscale image to 8, the better the randomness of the information distribution and the higher the security. The calculation equation is

\[
H(x) = -\sum_{i=0}^{2^N-1} (p(x_i) \log_2 p(x_i)),
\]

where \( N \) is the gray level and \( p(x_i) \) is the frequency of the gray value \( i \), the information entropy of the plaintext image and ciphered image of Lena, Peppers, and Cameraman is shown in Table 4. The information entropy of the ciphered image is 7.99749, 7.99749, and 7.99689, which are close to the ideal value and can well meet the security requirements.

5.6 Differential Attack. Differential attack is a kind of plaintext attack. The attacker will make very small changes to the plaintext to observe the changes of the ciphered and establish the association between the plaintext image and the ciphered image. There are two commonly used evaluation indicators for the ability to resist differential attacks: The

<table>
<thead>
<tr>
<th>Ciphered image</th>
<th>Lena</th>
<th>Peppers</th>
<th>Cameraman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Var</td>
<td>5156.719</td>
<td>5289.979</td>
<td>5154.814</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Image</th>
<th>Lena</th>
<th>Peppers</th>
<th>Cameraman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext</td>
<td>40394</td>
<td>36778</td>
<td>113650</td>
</tr>
<tr>
<td>Ciphered</td>
<td>228.0703</td>
<td>228.4453</td>
<td>281.1953</td>
</tr>
</tbody>
</table>

Table 1: Histogram analysis of variance results.

Table 2: \( \chi^2 \) test results.
Figure 10: Correlation of Lena plaintext images in three directions. (a) Horizontal direction; (b) vertical direction; (c) diagonal direction.

Figure 11: Correlation of Lena ciphered images in three directions. (a) Horizontal direction; (b) vertical direction; (c) diagonal direction.

Figure 12: Correlation of Peppers plaintext images in three directions. (a) Horizontal direction; (b) vertical direction; (c) diagonal direction.

Figure 13: Correlation of Peppers ciphered images in three directions. (a) Horizontal direction; (b) vertical direction; (c) diagonal direction.
number of Pixels Change Rate (NPCR) and Unified Average Intensity (UACI) [33]. The values of NPCR and UACI are calculated using the following two equations:

\[
\text{NPCR} = \left( \frac{\sum c_1(i, j) \neq c_2(i, j) \cdot 100}{M \cdot N} \right),
\]

\[
\text{UACI} = \left( \frac{\sum (c_1(i, j) - c_2(i, j))/255 \cdot 100}{M \cdot N} \right),
\]

where \(c_1\) is a plaintext image, and \(c_2\) is a ciphered image; if \(c_1(i, j) = c_2(i, j)\), then there is \(D(i, j) = 0\); otherwise \(D(i, j) = 1\).

Generally, the closer the theoretical value of NPCR is to 99.6094\% and the closer the theoretical value of UACI is to 33.4635\%, the better the algorithm resists differential attacks. In this paper, when calculating the two values, the pixel values of \(c_1(1, 1), c_1(256, 256)\) and \(c_2(1, 1), c_2(256, 256)\) are changed for an image each time, and the results are shown in Table 5. Every time a pixel of the image is changed, the NPCR and UACI obtained are close to the theoretical values.

By comparing with literature [32–34], we found that our algorithm has better security and ability to resist related attacks.

### 5.7. Four Common Attack Methods

Kerckhoff principle [34] that is the only thing that should be kept secret in a cryptographic system is the key, and the cryptographic algorithm should be made public. If a cryptographic system needs to be kept secret, the more possible weaknesses will be. Therefore, the cryptanalyst may know the design and work of other cryptographic systems except for the secret key. There are four types of attacks [35]: (1) only ciphered: the cracker only

#### Table 3: Correlation coefficient.

<table>
<thead>
<tr>
<th>Image</th>
<th>Horizontal direction</th>
<th>Vertical direction</th>
<th>Diagonal direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena plaintext</td>
<td>0.9385</td>
<td>0.9682</td>
<td>0.9129</td>
</tr>
<tr>
<td>Lena ciphered</td>
<td>0.0022</td>
<td>−0.0002</td>
<td>0.0044</td>
</tr>
<tr>
<td>Ref. [32]</td>
<td>0.9718</td>
<td>0.9526</td>
<td>0.9419</td>
</tr>
<tr>
<td>plaintext</td>
<td>0.0020</td>
<td>0.0052</td>
<td>0.0069</td>
</tr>
<tr>
<td>Ref. [33]</td>
<td>0.9876</td>
<td>0.9760</td>
<td>0.9626</td>
</tr>
<tr>
<td>ciphered</td>
<td>−0.0010</td>
<td>−0.0059</td>
<td>0.0072</td>
</tr>
</tbody>
</table>

#### Table 4: Image information entropy and comparison.

<table>
<thead>
<tr>
<th>Image</th>
<th>Lena</th>
<th>Peppers</th>
<th>Cameraman</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext</td>
<td>7.44459</td>
<td>7.53269</td>
<td>6.97190</td>
</tr>
<tr>
<td>Ciphertext</td>
<td>7.99749</td>
<td>7.99749</td>
<td>7.99689</td>
</tr>
</tbody>
</table>

Figure 14: Correlation of Cameraman plaintext images in three directions. (a) Horizontal direction; (b) vertical direction; (c) diagonal direction.

Figure 15: Correlation of Cameraman ciphered images in three directions. (a) Horizontal direction; (b) vertical direction; (c) diagonal direction.
<table>
<thead>
<tr>
<th></th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
<th>NPCR (%)</th>
<th>UACI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>c₁ (1, 1)</td>
<td></td>
<td></td>
<td>c₂ (256, 256)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lena</td>
<td>99.6093</td>
<td>33.5167</td>
<td>99.5895</td>
<td>33.5285</td>
<td>99.6503</td>
<td>33.4803</td>
</tr>
<tr>
<td>Peppers</td>
<td>99.5651</td>
<td>33.3992</td>
<td>99.5925</td>
<td>33.4094</td>
<td>99.6098</td>
<td>33.4536</td>
</tr>
<tr>
<td>Cameraman</td>
<td>99.5986</td>
<td>33.4562</td>
<td>99.5635</td>
<td>33.4692</td>
<td>99.6101</td>
<td>33.4602</td>
</tr>
</tbody>
</table>

**Figure 16:** Lena image cropping attack and noise attack results. (a) 1 randomly cropped area; (b) decrypted image corresponding to (a); (c) adding salt and pepper noise with variance of 0.1; (d) decrypted image corresponding to (c); (e) randomly cropped area 1 block + 0.1 salt and pepper noise; (f) decrypted image corresponding to (e).
has a string of ciphered; (2) select ciphered: the cracker gains access to the decryption machine; that is, it can select a ciphered character string to construct the corresponding plaintext string; (3) known plaintext: the cracker owns a string of plaintext and the corresponding cipher ciphered; (4) select the plaintext: the opponent obtains temporary

Figure 17: Baboon image cropping attack and noise attack results. (a) 1 randomly cropped area; (b) decrypted image corresponding to (a); (c) adding salt and pepper noise with variance of 0.1; (d) decrypted image corresponding to (c); (e) randomly cropped area 1 block + 0.1 salt and pepper noise; (f) decrypted image corresponding to (e).
Figure 18: Boats image cropping attack and noise attack results. (a) Random cropping area 1 block; (b) decrypted image corresponding to (a); (c) adding salt and pepper noise with variance of 0.1; (d) decrypted image corresponding to (e); (e) randomly cropped area 1 block + 0.1 salt and pepper noise; (f) decrypted image corresponding to (e).
access to the encryption machine. Therefore, he can select a plaintext string and construct the corresponding ciphered string. From the perspective of four typical attacks, the plaintext attack is the most powerful attack. If our algorithm can resist this attack, it can also resist several other attacks. The algorithm is sensitive to the initial values $x_0, x_1, x_2$, and control parameters $\mu_0, \mu_1, \mu_2$, and if one of the values changes, then $K^0 = \{k^0_1, k^0_2, \ldots, k^0_{M \times N}\}$, $K' = \{k'_1, k'_2, \ldots, k'_{M \times N}\}$, $P' = \{p'_1, p'_2, \ldots, p'_{M \times N}\}$, $S = \{s_1, s_2, \ldots, s_{M \times N}\}$ will be completely different. The sequence $K^2 = \{k^2_1, k^2_2, \ldots, k^2_{M \times N}\}$, $Q = \{q_1, q_2, \ldots, q_{M \times N}\}$ generated in the diffusion stage will also be completely different. This means that different images have different sequences of encryption operations to obtain different encrypted images. Therefore, the algorithm can resist plaintext/ciphered attacks.

5.8. Robustness Analysis. During the transmission process, the encrypted image may be affected by noise or loss of information. In order to verify the robustness of the encryption algorithm proposed in this article, this article performs cropping attacks and noise addition attacks on encrypted images. In the experiment, different regions of the image were cropped, and salt and pepper noise with a variance of 0.1 was added. As shown in Figures 16–18, respectively, it is shown that when Lena, Baboon, and Boats images are attacked by different degrees of noise, the decrypted images can still be distinguished. Experimental results show that the algorithm proposed in this paper has good antishear and antinoise capabilities and has good robustness.

6. Conclusion

This paper proposes a chaotic system image encryption algorithm based on power exponent operation, combined with one-dimensional Sine chaotic system, and proposes a brand new chaotic system—HPECS-SS. Comparing this system with the ordinary one-dimensional chaotic systems logistic and Sine, it is found that HPECS-SS has a larger parameter range and higher complexity. At the same time, based on HPECS-SS, a new encryption image algorithm is proposed. Experimental results show that the ciphered information entropy, NPCR, and UACI obtained by the algorithm are close to ideal values, which can effectively resist differential attacks and meet the security requirements well. The encryption and decryption in this article are the study of the standard $256 \times 256$ grayscale image. The later work plans to use the RGB three-channel image input method to realize the colour image encryption research. [36].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This research was supported by Henan Province Science and Technology Research Project nos. 212102210407 and 192102210133 and Key R&D and Promotion Projects in Henan Province, nos. 212102210425 and 202102210182.

References


