Hindawi
Security and Communication Networks
Volume 2020, Article ID 9721675, 14 pages
https://doi.org/10.1155/2020/9721675

*Research Article*

# Image Encryption Scheme Based on a Generalized Arnold Map and RSA Algorithm

**Kaixin Jiao, Guodong Ye, Youxia Dong, Xiaoling Huang, and Jianqing He**

*Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China*

Correspondence should be addressed to Guodong Ye; guodongye@hotmail.com

Received 9 January 2020; Revised 10 May 2020; Accepted 18 May 2020; Published 4 June 2020

Academic Editor: Angel M. Del Rey



This study proposes a new image encryption scheme based on a generalized Arnold map and Rivest–Shamir–Adleman (RSA) algorithm. First, the parameters of the generalized Arnold map are generated by an asymmetric encryption-system RSA algorithm, and the keystream is produced iteratively. To change the distribution of pixel values, the image data are hidden by XOR diffusion. Second, both rows and columns of the image are cyclically confused to hide the image data again. Then, the additive mode diffusion operation is performed to realize third-layer hiding for image content. The overall diffusion and confusion operations are conducted twice to obtain the final cipher image. Test results prove that the encryption scheme proposed in this study is effective and has strong antiattack capabilities and key sensitivity. In addition, because the scheme security relies on the RSA algorithm, it has high security.

## 1. Introduction

With the rapid development and popularization of computer-network and multimedia technology, computer networks have become important media for timely release of information. To display information content more intuitively and realistically, digital images are the most direct means of expressing information. Because images can reveal sensitive business, military, medical, and political issues, methods to protect their transmission and storage on public networks in the fields of encryption and information security have attracted greater attention than ever before. Classic cryptography provides better encryption and decryption algorithms for one-dimensional data streams. Examples include the data encryption standard, advanced encryption standard, and other cryptosystems. However, the special properties of digital images, including large data volume, high redundancy, and strong correlation, between adjacent pixels make traditional block ciphers less efficient when processing image data [1].

Accordingly, image encryption algorithms based on Arnold transform [2], double random phase coding [3], chaotic systems [4–6], compressed sensing [7–10], and other technologies have been proposed. Chaotic systems are widely used in image encryption because of basic characteristics such as sensitivity to initial conditions, pseudorandomness, ergodicity, and nonperiodicity. The image information encryption scheme based on chaos uses the random noise characteristics of a chaotic time series to encrypt the image data. Its main operational steps include image pixel diffusion and pixel position confusion. An efficient pixel-level image encryption algorithm was presented by Ye et al. [11], which enhanced the connection between position shuffling of pixels and the changes to gray values as compared to the traditional permutation-diffusion architecture. Zhu et al. [12] proposed an image cryptosystem based on a confusion and diffusion structure that uses an Arnold cat map for bit-level arrangement and a logistic map for diffusion. Addressing the insensitivity of traditional permutation and diffusion operations to pure image changes, Zhang et al. [13] proposed a lightweight bit-level confusion and cascade cross circular diffusion, which diffuses a small change in the plane image to the whole image with fewer rounds to enhance the security of the cryptographic system and reduce computational redundancy in the traditional architecture. Liu et al. [14] designed a color image

encryption algorithm by using Arnold and discrete cosine transforms. The color image RGB components are confused by the Arnold transform, and the confused RGB components are randomly exchanged and mixed under the control of the matrix defined by a random angle. Unlike many image cryptosystems that perform permutation at the pixel level, the study in [15] used three-dimensional puzzle and chaotic maps to further promote diffusion and confusion. The method performs permutation at both the bit and pixel levels to provide additional confusion.

However, most of the aforementioned methods are types of symmetric cryptosystems, where the encryption and decryption keys are the same. This may cause problems related to security [16] and key management [17]. To overcome the disadvantages of symmetric cryptography, many asymmetric encryption algorithms have been proposed [18–21] that use public and private keys for encryption and decryption, respectively. The study in [22] proposed an asymmetric cryptosystem based on phase-truncated Fourier transform. Through phase truncation in the Fourier transform, two random phase keys are used as the public key to generate asymmetric ciphertext as real values and stationary white noise. Deng and Zhao [23] combined the color components multiplied by three random phase keys into a grayscale image through convolution. They then encoded it into a real-valued grayscale ciphertext using an asymmetric cryptosystem. The decryption key is generated during the encryption process and is different from the encryption key. Rakheja et al. [24] proposed an asymmetric hybrid cipher scheme for coherent superposition and random decomposition in a hybrid multiresolution wavelet domain using a four-dimensional hyperchaotic structure. The parameters and preliminary conditions of the four-dimensional hyperchaotic structure together with the fractional order expand the key space and consequently provide the system with additional strength. Chen et al. [25] proposed a color image enhancement asymmetric cryptosystem based on equal modulus decomposition (EMD) and created an effective one-way trapdoor function through EMD. In addition, to improve the security, the red-green-blue (RGB) components of color images were confused by using a Baker map. Wang et al. [26] proposed a double-image encryption technology based on an asymmetric algorithm. During the nonlinear encryption process, the image is encoded as amplitude ciphertext, and two phase-only masks generated based on phase truncation are retained as the decryption key.

The RSA algorithm is a type of public key cryptosystem. Its security is based on the difficulty of decomposing large integers into prime factors. Therefore, it is widely used in the field of image encryption [27, 28]. Liu et al. [29] proposed a digital image watermarking model based on the scrambling algorithm logistic and RSA asymmetric encryption algorithm, which ensure the security of hidden data based on a large embedding amount, strong robustness, and high computing efficiency. The logistic and RSA encryption algorithms are applied to the watermark image, and the image is decomposed by discrete wavelet transform and singular value decomposition, and then the watermark is embedded into the low-frequency subband of the host. To enhance the strength of the cryptosystem and provide higher security, the scheme in [30] uses the RSA algorithm and public key to encrypt the plain image to generate a cipher image. It then re-encrypts the cipher image to perform double encryption through chaotic synchronization.

Different from the commonly used method of image Arnold scrambling, this study uses the generalized form of the Arnold formula to generate the key flow. The image is first XOR diffused. The row and column directions are confused, and then the image information is hidden again by point diffusion.

The remainder of this paper is organized as follows. Section 2 introduces the RSA algorithm and generalized Arnold map, and Section 3 describes the proposed image encryption and decryption process. Section 4 presents the experimental results, and Section 5 analyzes and tests the effects of the algorithm. Section 6 gives a conclusion.

## 2. Related Works

Chaotic sequence is a kind of pseudorandom sequence with good performance, which has abundant sources, simple generation method, and an almost undecipherable encryption sequence and can be determined by mapping function, generation rules, and initial conditions. Because of the good characteristics of chaotic system, it has been widely used in the field of image encryption.

Chen et al. [31] proposed a new simple pixel-dependent swap-aliasing method, which can achieve considerable diffusion in the process of permutation. The self-correlation non-linear pixel-exchange aliasing method is used to generate completely different aliasing images, which speeds up the propagation process of the cryptosystem and reduces the time-consuming work of the diffusion part. Zhang [32] proposed an image encryption algorithm related to plaintext, which combined two diffusion operations and a transform related to plaintext to encrypt the image and used a hyperchaotic system to generate the key stream. Hua et al. [33] proposed an image encryption algorithm based on two-dimensional (2D) logic-sinusoidal coupling mapping (LSCM) and classic obfuscation-diffusion structure. The algorithm has better ergodicity, more complex behavior, and larger chaotic range. Chai et al. [34] proposed a color image encryption algorithm based four-wing hyperchaotic system and DNA sequence operation. The work proposed by Hua et al. [35] used the generated cosine transform chaotic map to further propose an image encryption scheme. The generated chaotic map exhibits more complicated chaotic behavior than the existing chaotic map.

In order to improve the robustness to common attacks, Yu et al. [36] proposed an image encryption algorithm based on phase-truncated short time fractional Fourier transform (PTSTFrFT) and hyperchaotic system. The feedback system is used to design the diffusion operation, which improves the anti-interference ability of the system. Due to the hyperchaotic system, the proposed image encryption algorithm has a sufficiently large key space and high sensitivity to the key. Huang et al. [37] proposed a nonlinear optics image encryption algorithm based on Logistic map. The phase

truncation and the bitwise XOR operation, as non-linear processes, improve the robustness of the presented multi-image encryption scheme against the chosen-plaintext attack.

More scholars now combine chaotic systems with current popular technologies, such as compressed sensing, neural networks, electronic communications, and DNA coding. Compressed sensing can compress the image data information while sampling the image and then use the reconstruction algorithm to complete the restoration of the image information. For example, in [38], Liu et al. proposed an encryption algorithm in which the compressed image obtained using measurement matrix is scrambled with the Arnold cat map. The scrambled image is encrypted with double random phase encoding (DRPE). A novel image compression and encryption scheme was put forward based on wavelet packet transform and chaotic system, where logistic map was employed to generate the initial values of Chen's chaotic system to control the confusion and diffusion of the input image [39]. Zhou et al. [40] proposed an efficient image compression and encryption scheme based on hyperchaos system and two-dimensional compressed sensing. The proposed cryptosystem reduces the amount of data transmitted and simplifies the nonlinear distribution of keys.

The DNA computing process has lots of good characteristics [41] such as massive parallelism, huge storage, and ultra-low-power consumption. Many researchers have combined the properties of chaos and DNA encoding techniques to enhance the security of images in all aspects [42, 43]. Chai et al. [44] combined the memory hyperchaotic system, cellular automata, and DNA sequence operations to develop an encryption system for grayscale images. The calculation of this system is relatively complicated, but it can resist known plaintext and select plaintext attacks. Wu et al. [45] proposed an image encryption procedure based on CML (Coupled Map Lattice) and DNA encryption. The method has an extended hamming distance calculation to improve the ability to resist plaintext attacks. In [46], the encryption scheme combines chaotic image encryption technology and DNA sequence manipulation technology. A new Mandelbrot set based conditional shift algorithm is introduced to apply confusion effectively on R, G, and B channels.

It can be seen that chaotic systems have been widely used in image encryption. However, many image encryption algorithms have defects in the specific process, such as the difficulty to exchange secre keys. Therefore, this paper combines a chaotic system with an asymmetric encryption algorithm and uses the generated key stream to scramble and diffuse the image to solve the exchange key problem.

## 3. Background

*3.1. RSA Algorithm.* RSA public key cryptography was first proposed by Rivest, Shamir, and Adleman. It is based on the Euler theorem of number theory, and the security is based on the difficulty of factoring large integers. RSA can be used for both encryption and digital signatures and is secure, easy to understand, and easy to implement. The RSA algorithm encryption and decryption processes are given by Algorithm 1.

The algorithm is asymmetric because different keys are used during encryption and decryption. The plaintext data are encrypted using the public key, and the receiver decrypts the ciphertext with its own private key to obtain the plaintext data. The private key is only known to the receiver, which reduces the transmission of the key in the channel.

*3.2. Generalized Arnold Map.* The Arnold map is a type of nonlinear map commonly known as a "cat map," which is defined as follows:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{1}$$

where $(x_i, y_i)$ is the position of the pixel before the exchange and $(x_{i+1}, y_{i+1})$ is the position of the transformed pixel. The pixel scrambling algorithm based on Arnold mapping is shown in Algorithm 2.

After stretching, the Arnold map is referred to as a generalized Arnold map, which is defined as

$$\begin{cases} x_{i+1} = x_i + by_i \bmod 1, \\ y_{i+1} = ax_i + (ab+1)y_i \bmod 1. \end{cases} \tag{2}$$

The chaotic sequences $\{x_k\}_{k=0}^{\infty}$ and $\{y_k\}_{k=0}^{\infty}$ generated by (2) are nonperiodic, nonconvergent, and pseudorandom [47] and are given by parameters $a$, $b$, $x_0$, and $y_0$. The largest Lyapunov characteristic exponent of the map is $\lambda = 1 + ((ab + \sqrt{a^2b^2 + 4ab})/2) > 1$. That is to say, the map is always in chaotic for parameters. For example, Figure 1 shows its chaotic behavior when $a = 1$, $b = 1$, $x_0 = 0.3044$, and $y_0 = 0.2691$.

In order to further test the properties of chaotic sequences, when parameter $a = 4b = 8$, $x_0 = 0.5$, and $y_0 = 0.9$, the system parameters are unchanged; change the initial value $x_0$ or $y_0$ by 0.000001 to obtain two chaotic sequences. In the experiment, the first 50 sequence values of chaotic sequences are selected for comparison, and the comparison results are shown in Figure 2. The solid line represents the chaotic sequence value when the initial value has not changed, and the dashed line represents the chaotic sequence value after the initial value has changed slightly by 0.000001. The experimental results show that the chaotic sequence generated by the chaotic system has very sensitive.

## 4. Proposed Image Encryption Scheme

*4.1. Image Encryption Process.* This study implements a new asymmetric image encryption scheme using the generalized Arnold map, RSA algorithm, and confusion and diffusion technology. Algorithm 3 is the pseudocode of our image encryption algorithm. The flow of image encryption is presented in Figure 3, where the specific encryption process is described as follows:

Input: choose different large primes $p$; $q$
(1) $\varphi(n) = (p-1)(q-1)$
(2) $n = p \times q$
(3) Random selection $e$, $1 < e < \varphi(n)$, and $\gcd(\varphi(n), e) = 1$
(4) Calculating the private key $d$, $d \cdot e = 1 \bmod \varphi(n)$, $d = e^{-1} (\bmod \varphi(n))$
(5) Encryption method: for each plaintext grouping $m$, perform encryption operation, namely, $c = m^e \bmod n$
(6) Decryption method: the decryption operation of the ciphertext packet is: $m = c^d \bmod n$

Algorithm 1: RSA encryption and decryption algorithm.

Input: $P$ (plain image), $a$, $b$;
Output: $C$ (confused image)
(1) Read the image $P$ and get its size $N \times N$;
(2) Let img = $P$ and $C$ be a zero image with the same size of $P$;
(3) For each row $x$ and column $y$, do:
(4) $X = (x + by) \bmod N + 1$;
(5) $Y = (ax + (ab+1)y) \bmod N + 1$;
(6) $C(X, Y) = \text{img}(x, y)$;
(7) Return

Algorithm 2: Arnold confusion algorithm.

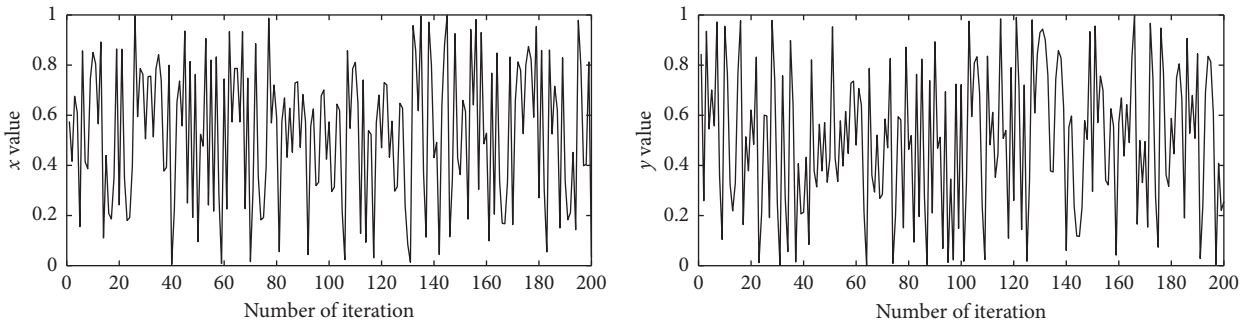


Figure 1: Chaotic sequence: (a) $x$ value; (b) $y$ value.

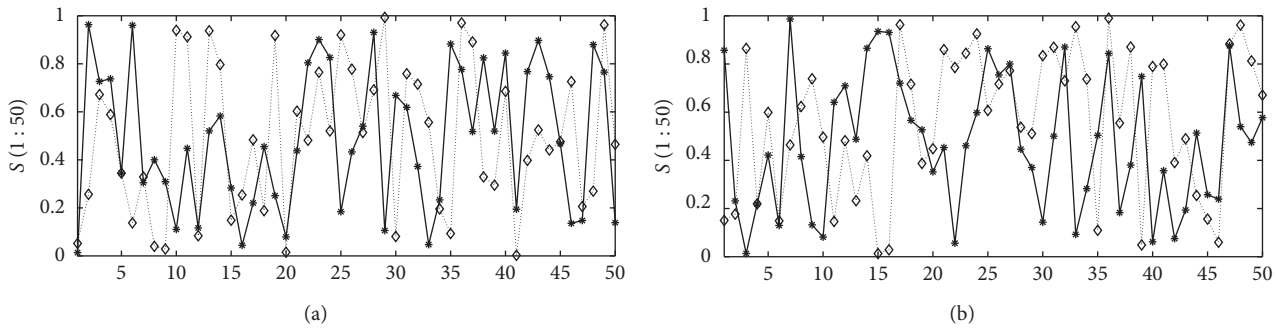


Figure 2: Difference diagram of chaotic sequence. (a) The solid line: $x_0 = 0.5$; the dashed line: $x_0 = 0.500001$. (b) The solid line: $y_0 = 0.9$; the dashed line: $x_0 = 0.900001$.

Step 1: select prime numbers $p$ and $q$, and calculate $n = p \times q$, $\varphi(n) = (p-1)(q-1)$

Step 2: generate private key $d$ and public key $e$ using the RSA algorithm

Step 3: four positive integers ($x_{01}$, $x_{02}$, $x_{03}$, and $x_{04}$) are randomly selected as confidential information, and equation (3) is used to calculate $y_{0i}, i = 1, 2, 3, 4$

Step 4: public ciphertext $c_i = y_{0i}{}^e \bmod n, i = 1, 2, 3, 4$ is calculated using public key $e$, and then equation (4) is used to calculate the parameter pairs $a$ and $b$ of the Arnold map:

$$\begin{cases} y_{01} = x_{01} + x_{02}, \\ y_{02} = x_{02} + x_{03}, \\ y_{03} = x_{03} + x_{04}, \\ y_{04} = x_{01} + x_{04}, \end{cases} \tag{3}$$

$$\begin{cases} a_1 = \mathrm{fix}\left(x_{01} + \mathrm{sqrt}\left(\log\left(c_1 + y_{01}\right)\right)\right), \\ b_1 = \mathrm{fix}\left(x_{02} + \mathrm{sqrt}\left(\log\left(c_2 + y_{02}\right)\right)\right), \\ a_2 = \mathrm{fix}\left(x_{03} + \mathrm{sqrt}\left(\log\left(c_3 + y_{03}\right)\right)\right), \\ b_2 = \mathrm{fix}\left(x_{04} + \mathrm{sqrt}\left(\log\left(c_4 + y_{04}\right)\right)\right). \end{cases} \tag{4}$$

Step 5: substitute parameters $a_1$, $b_1$, $a_2$, and $b_2$ into the generalized Arnold map equation to generate chaotic sequences $s$ and $r$, and convert the generated values into the range of 0 to 255:

$$\begin{aligned} S &= \mathrm{mod}\left(\mathrm{floor}\left(\left(s + 100\right) \times 10^{14}\right), 256\right), \\ R &= \mathrm{mod}\left(\mathrm{floor}\left(\left(r + 100\right) \times 10^{14}\right), 256\right). \end{aligned} \tag{5}$$

Step 6: record the plain image as $P$ and perform the following XOR diffusion operation with the generated key stream $S$ to obtain image $A$:

$$A_i = A_{i-1} \oplus P_i \oplus S_i, \tag{6}$$

where $A_i$, $P_i$, and $S_i$ represent the elements of $A$, $P$, and $S$.

Step 7: transform $S$ into a matrix. Then, take the first row and first column of the image matrix $S$ and conduct cyclic scrambling of the row and column directions of image $A$ to obtain image $B$

Step 8: image $B$ and chaotic sequence $R$ are used to perform an additive mode diffusion operation to obtain image $C$ as

$$C_i = C_{i-1} + B_i + R_i \bmod 256, \tag{7}$$

where $C_i$, $B_i$, and $R_i$ represent the elements of $C$, $B$, and $R$.

Step 9: after two rounds of calculation, the final encrypted image $E$ is obtained.

As to the color image, it can be treated as three gray images by three channels R, G, and B. So, the encryption is the same for each channel.

*4.2. Image Decryption Process.* Image decryption is the reverse process of encryption, Algorithm 4 is the pseudocode of image decryption algorithm, and its steps involve the following.

Step 1: public ciphertext information $c_i, i = 1, 2, 3, 4$ is decrypted with private key $d$, that is, $y_{0i} = c_i^d \bmod n, i = 1, 2, 3, 4$. Then, parameter pairs $a$ and $b$ of the Arnold map are generated according to (3) and (4).

Step 2: when the two pairs of parameters are substituted into the generalized Arnold map equation, the chaotic sequences $s'$ and $r'$ are generated, and the generated values are transformed into the range from 0 to 255:

$$\begin{aligned} S' &= \mathrm{mod}\left(\mathrm{floor}\left(\left(s' + 100\right) \times 10^{14}\right), 256\right), \\ R' &= \mathrm{mod}\left(\mathrm{floor}\left(\left(r' + 100\right) \times 10^{14}\right), 256\right). \end{aligned} \tag{8}$$

Step 3: the cipher image $E$ and chaotic sequence $R'$ are added to obtain the image $C'$ using the operation of adding modulus inverse diffusion, described by

$$C_i' = 2 \times 256 + E_i - E_{i-1} - R_i' \bmod 256, \tag{9}$$

where $C_i'$, $E_i'$, and $R_i'$ represent the elements of $C'$, $E'$, and $R'$.

Step 4: transform $S'$ into a matrix. Then, take the first row and first column of the image matrix to perform the cyclic confusion of the rows and columns of image $C'$ to obtain image $B'$.

Step 5: perform the XOR diffusion operation with image $B'$ and $S'$ to obtain image $A'$, described by

$$A_i' = B_{i-1}{}' \oplus B_i' \oplus S_i', \tag{10}$$

where $A_i'$, $B_i'$, and $S_i'$ represent the elements of $A'$, $B'$, and $S'$.

Step 6: plain image $P'$ is obtained after two rounds of the decryption operation.

## 5. Experimental Results

This paper selects some different images from the USC-SIPI and Kodak databases. The Windows 10 operating system was used with the MATLAB R2017b software. An AMD Ryzen 7 1700 eight-core processor was used, and 8 GB of RAM was required to simulate the work. For the experimental process, the private key consisted of large prime numbers $p = 911$, $q = 997$, and $d = 147547$. Positive integers were separately selected as $x_{01} = 3$, $x_{02} = 5$, $x_{03} = 7$, and $x_{04} = 11$. The public key consisted of $e = 43$, $c_1 = 525020$, $c_2 = 518815$, $c_3 = 745188$, and $c_4 = 658943$. The obtained results were as follows: $a_1 = 6$, $b_1 = 8$, $a_2 = 10$, and $b_2 = 18$. The results for the test image encryption and decryption are shown in

**Input**: original image $P$, secret keys $x_{01}, x_{02}, x_{03}, x_{04}$
Read the image size $M \times N$
Calculate the $a, b$ for Arnold map by equations (3) and (4) together with RSA and $x_{01}, x_{02}, x_{03}, x_{04}$
Generate the key streams $S$ and $R$ by equation (2)
Take a row and a column from $S$ and sort them, then get $X$ and $Y$
$B = P \oplus S$; //perform XOR diffusion operations
for $i = 1 : M$
  $D(X(i), :) = B(i, :)$; //confusion on the row direction
end
for $i = 1 : N$
  $E(:, Y(i)) = D(:, i)$; //confusion on the column direction
end
$C = \mathrm{mod}(E + R, 256)$; //perform additive mode diffusion operations
**Output**: encryption image $C$

Algorithm 3: Pseudocode of image encryption.

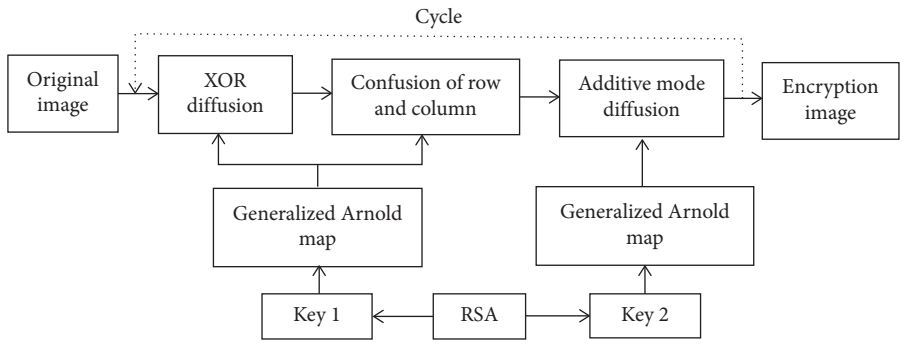


Figure 3: Flow of the proposed image encryption algorithm.

**Input:** encryption image $C$, public information $c_i, i = 1, 2, 3, 4$
Read the image size $M \times N$
Use private key $d$ to decrypt to get $y_{0i}, i = 1, 2, 3, 4$
Calculate the $a, b$ for Arnold map by equations (3) and (4)
Generate the key stream $S'$ and $R'$ by equation (2)
Take a row and a column from $S'$ and sort them, then get $X'$ and $Y'$
$C' = \mathrm{mod}(2 \times 256 + E - R')$; //the inverse operation of additive mode diffusion
for $i = 1 : M$
  $E'(i, :) = C'(X'(i):)$; //confusion decryption on the row direction
end
for $i = 1 : N$
  $B'(:, i) = E(:, Y'(i))$; //confusion decryption on the column direction
end
$A' = B' \oplus S'$; //perform XOR diffusion operations
**Output:** original image $A'$

Algorithm 4: Pseudocode of image decryption.

Figure 4 with two rounds. The encrypted image in Figures 4(i)–4(p) reveals that no information could be retrieved from it. The decrypted image (Figures 4(q)–4(x)) also shows that the plain image information could be correctly decrypted and restored. This proves that the proposed cryptosystem provides good encryption results and is effective for digital images. Table 1 shows the time cost used by different size image. It can be seen that the result is slightly big due to the RSA algorithm. However, it can also be accepted.

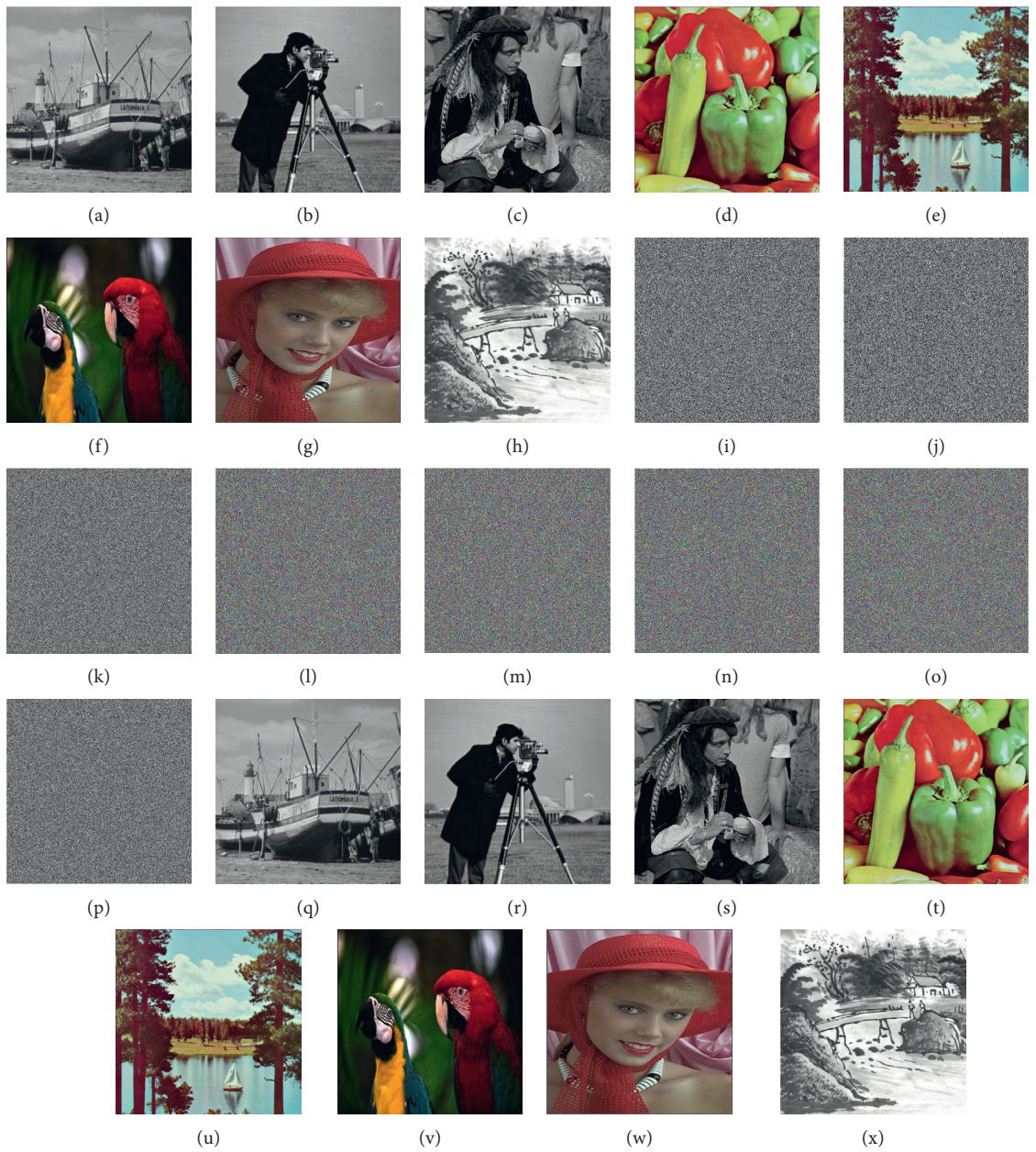


Figure 4: Results of the test images. Plain images of (a) boat; (b) man; (c) male; (d) peppers; (e) sailboat; (f) bird; (g) woman; (h) landscape. Encrypted images of (i) boat; (j) man; (k) male; (l) peppers; (m) sailboat; (n) bird; (o) woman; (p) landscape. Decrypted images of (q) boat; (r) man; (s) male; (t) peppers; (u) sailboat; (v) bird; (w) woman; (x) landscape.

Table 1: Time cost analysis.

| Image | Key stream generation Time (s) | Confusion-diffusion Time (s) | One round Time (s) |
|---|---|---|---|
| Boat (512*512) | 0.256226 | 0.241599 | 0.241728 |
| Male (1024*1024) | 0.550868 | 2.227201 | 2.227410 |

## 6. Analysis of Encryption Effects

*6.1. Histogram Analysis.* A histogram is used to display the distribution of pixel intensity in an image. An ideal encrypted image typically has a uniform frequency distribution and will provide no useful statistical information to the attacker. Figure 5 shows the histogram distribution of some test images before and after encryption, showing the

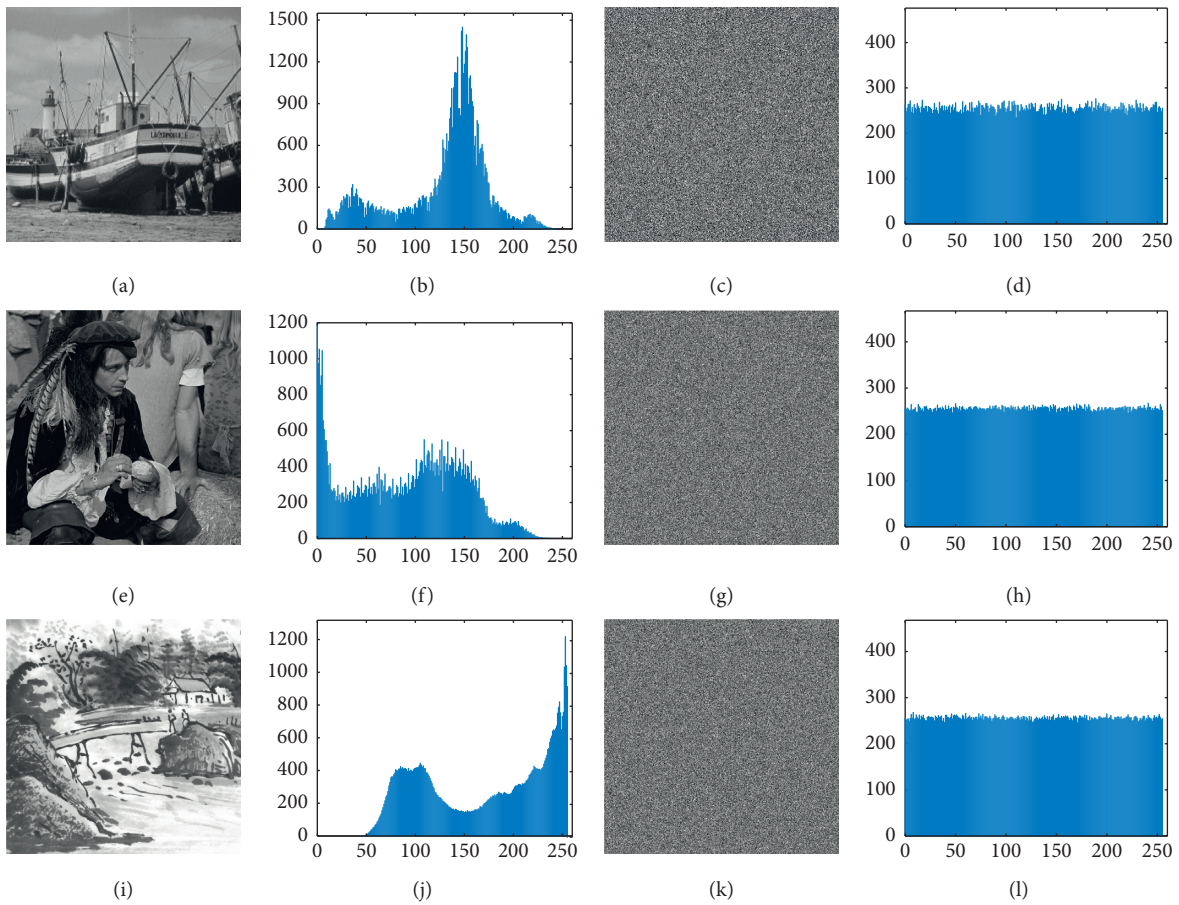


Figure 5: Histogram test: (a) plain image of boat; (b) histogram of the plain image boat; (c) cipher image of boat; (d) histogram of the cipher image boat; (e) plain image of male; (f) histogram of the plain image male; (g) cipher image of male; (h) histogram of the cipher image male; (i) plain image of landscape; (j) histogram of the plain image landscape; (k) cipher image of landscape; (l) histogram of the cipher image landscape.

uniformity of gray values in the results. Simultaneously, a chi-squared test can be used to evaluate the uniformity of the histogram, which is calculated as

$$\chi^2 = \sum_{L=0}^{255} \frac{(O-E)^2}{E}, \tag{11}$$

where $L$ is the intensity level and $O$ and $E$ are the observed and expected values for each pixel in the encrypted image, respectively. The uniformity of histogram is assessed with the help of the chi-squared test. Table 2 shows the histogram uniformity results of the test images based on the $\chi^2$ test, in which the color images take the average values of three channels. From Table 2, all test images have passed chi-squared detection, proving the uniformity of histogram. Hence, it is evident that the redundancy of plain images is concealed which confirmed the failure of statistical attack [48].

*6.2. Correlation Coefficient.* The correlation coefficient is a linear correlation between adjacent pixels in an image. When the two-dimensionality of the image is considered, the correlation is derived from the horizontal, vertical, and diagonal directions. Secure encryption schemes should reduce the correlation between adjacent encrypted image pixels to prevent statistical analysis attacks. To evaluate the correlation between two pixels, the adjacent pixel pairs in three directions are randomly selected from the normal and encrypted images for calculation. The calculation formula is defined as

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{12}$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right), \tag{13}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{14}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2, \tag{15}$$

where $r_{xy}$ is the correlation coefficient, $x$ and $y$ are the gray values of two adjacent pixels, and $N$ is the total logarithm of

Table 2: Histogram uniformity evaluation based on the $\chi^2$ test.

| Image | Plain-image | Cipher-image | Result |
|---|---|---|---|
| Boat | 383969.6875 | 239.3281 | Pass |
| Man | 392972.1914 | 241.9551 | Pass |
| Male | 709340.6801 | 257.8115 | Pass |
| Peppers | 340999.4414 | 267.2064 | Pass |
| Sailboat | 223807.8535 | 256.8639 | Pass |
| Bird | 871600.3639 | 251.2643 | Pass |
| Woman | 263568.7500 | 259.0684 | Pass |
| Landscape | 710898.8340 | 239.4194 | Pass |

$(x_i, y_i)$. The correlation coefficient value is between −1 and +1. For an effective encryption algorithm, the correlation coefficient value of the encrypted image should be close to 0 [49]. The correlation coefficient between the original image (Boat) and the corresponding encrypted image is shown in Figure 6. Table 3 calculates the correlation coefficients of some images in test images from horizontal, vertical, and diagonal directions. For color images, it is necessary to consider three different channels. Table 4 takes peppers image as an example to analyze the correlation coefficient between the original image and the encrypted image. Table 5 compares the correlation coefficient results of man images in different encryption algorithms. The test results show that the proposed scheme breaks the strong correlation in the original image and can effectively resist attacks.

*6.3. Information Entropy.* In information theory, entropy information can be defined as the uncertainty of the information content. This can then be used to measure the randomness of data sequences. It can be defined as

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i)\log_2\frac{1}{p(m_i)}, \tag{16}$$

where $p(m_i)$ is the probability of $m_i$ and $n$ is the number of bits of $m_i$. For digital images with $2^8$ grayscale levels, the maximum information entropy is 8. The higher the entropy value of the encrypted image, the more uniform is the pixel value distribution. Among them, local Shannon entropy measures image randomness by calculating the sample mean of Shannon entropy on multiple non-overlapping and randomly selected image blocks, so it can overcome the shortcomings of global information entropy such as inaccuracy, inconsistency, and low efficiency [50]. Table 6 shows the information entropy of the test image and the local entropy of the encrypted image. The information entropy value of color image is calculated as the average information entropy value of three channels. The results reveal that the entropy values of test images were close to the ideal values.

*6.4. Differential Attack Analysis.* Difference analysis evaluates the degree of sensitivity to ordinary images, where the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are two common indicators of attack resistance [51–53]. NPCR measures the rate of change of pixel values in a cipher image by changing one pixel value of the original image. The higher the value of UACI, the more sensitive is the cipher to changes in the plain image. Therefore, it has stronger resistance to a differential attack. It can be defined as

$$\mathrm{NPCR}(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{M\times N}\times 100\%, \tag{17}$$

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j), \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j), \end{cases} \tag{18}$$

$$\mathrm{UACI}(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j) - C_2(i,j)\right|}{M\times N\times T}\times 100\%, \tag{19}$$

where $M$ is the width of the image, $N$ is the height, and $T$ is the maximum allowable pixel value of the image. Here, $C_1$ is the encrypted image and $C_2$ is the encrypted image modified after one pixel value of the original image is changed. Table 7 shows the average NPCR and UACI values of the some test images. Table 8 lists the results of NPCR and UACI when the pixel values at different positions of the common image are changed. All values of NPCR and UACI of our method are close to ideal values 99.6094% and 33.4635%, respectively.

*6.5. Key Sensitivity Analysis.* To resist violent attacks, a password system should be highly sensitive. In this system, a slightly different key is used to encrypt the original image using the same encryption algorithm, with the remaining keys being unchanged. Key sensitivity tests were conducted as follows.

Suppose the initial set of keys used in the proposed cryptosystem is recorded as keys 1, denoted as

$$\text{keys1} = \{p, q, e, d, x_{01}, x_{02}, x_{03}, x_{04}, x', y', x_1', y_1'\}, \tag{20}$$

where the values of $p, q, d, x_{01}, x_{02}, x_{03}, x_{04}$ represent the private key (i.e., the secret information) and $e, x', y', x_1', y_1'$ represent the public key.

The initial key set keys 1 is used to encrypt the original image (boat) to obtain an encrypted image. Figure 7(a) shows the "boat" image, and Figure 7(b) shows an encrypted image. Suppose a value in keys 1 changes slightly, then keys 2 is expressed as

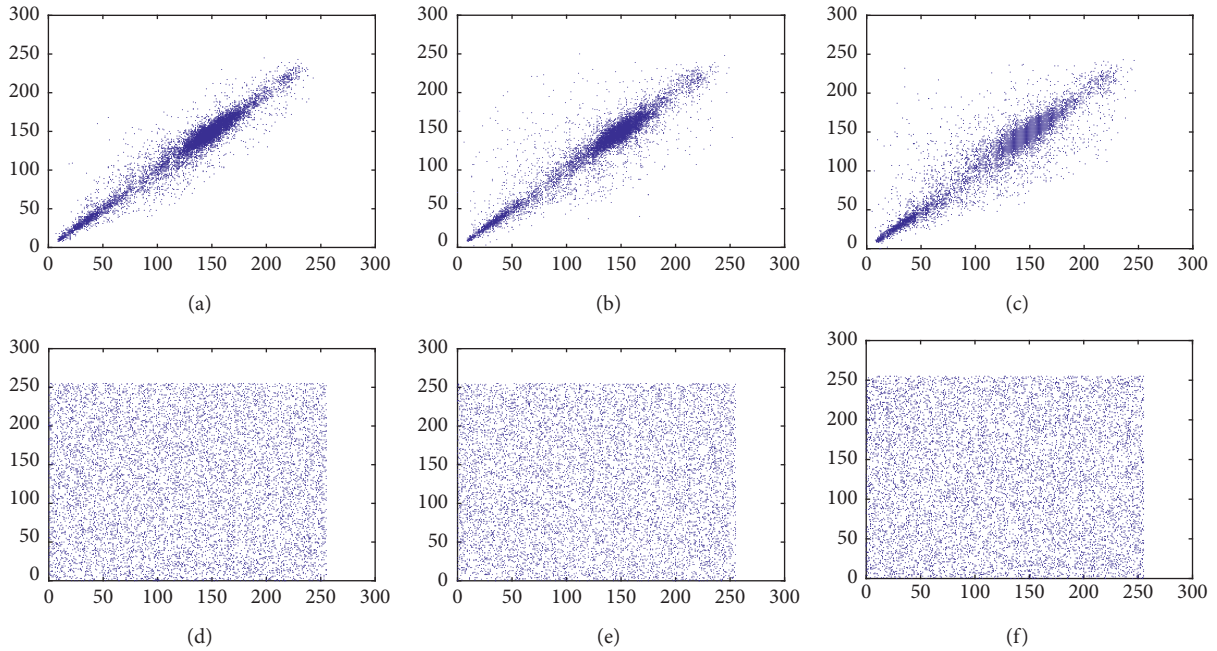


Figure 6: Correlation of two adjacent pixels in a plain image of 512 × 512 Boat in (a) horizontal; (b) vertical; and (c) diagonal directions. Correlation of two adjacent pixels in the cipher image: (d) horizontal; (e) vertical; and (f) diagonal directions.

Table 3: Correlation coefficients of different test images.

| Image | Plain-image | | | Cipher-image | | |
|---|---|---|---|---|---|---|
| | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Boat | 0.9379 | 0.9383 | 0.8790 | 0.0146 | 0.0026 | 0.0013 |
| Man | 0.9911 | 0.9850 | 0.9362 | 0.0065 | −0.0046 | −0.0017 |
| Male | 0.9182 | 0.9304 | 0.8746 | −0.0068 | 0.0163 | −0.0017 |
| Landscape | 0.5778 | 0.6379 | 0.5558 | −0.0035 | 0.0013 | −0.0053 |

Table 4: Coefficient correlation between the color peppers.

| | Plain-image | | | Cipher-image | | |
|---|---|---|---|---|---|---|
| | R | G | B | R | G | B |
| Horizontal | 0.9656 | 0.9803 | 0.9686 | −0.0143 | −0.0061 | 0.0052 |
| Vertical | 0.9649 | 0.9799 | 0.9683 | 0.0017 | 0.0063 | −0.0027 |
| Diagonal | 0.9582 | 0.9680 | 0.9478 | 0.0134 | −0.0085 | 0.0070 |

Table 5: Comparison of correlation coefficients of man image.

| Algorithm | Image | Cipher-image | | |
|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal |
| | Man | 0.9911 | 0.9850 | 0.9362 |
| Proposed | Encrypted man | 0.0065 | −0.0046 | −0.0017 |
| Ref. [5] | Encrypted man | 0.0198 | 0.0132 | 0.0032 |
| Ref. [10] | Encrypted man | 0.0685 | 0.0821 | 0.0821 |

$$\text{keys2} = \{p, q, e, d, x_{01} - 1, x_{02}, x_{03}, x_{04}, x', y', x_1', y_1'\}. \quad (21)$$

The original image is encrypted with keys 2 using the same encryption algorithm to obtain the other encrypted image shown in Figure 7(c). Figure 7(d) is a difference image

Table 6: The information entropy and local entropy of test images.

| Image | Plain-image | Cipher-image | Local shannon |
|---|---|---|---|
| Boat | 7.19137 | 7.99934 | 7.95559 |
| Man | 7.10904 | 7.99933 | 7.95658 |
| Male | 7.52374 | 7.99982 | 7.95709 |
| Peppers | 7.29780 | 7.99927 | 7.95268 |
| Sailboat | 7.38963 | 7.99929 | 7.95583 |
| Bird | 6.73746 | 7.99931 | 7.95701 |
| Woman | 7.24185 | 7.99929 | 7.95257 |
| Landscape | 7.45319 | 7.99984 | 7.95436 |

Table 7: Average NPCR and UACI of test images.

| Image | NPCR (%) | UACI (%) |
|---|---|---|
| Boat | 99.6094 | 33.4910 |
| Man | 99.6323 | 33.3144 |
| Male | 99.6538 | 33.4650 |
| Landscape | 99.6628 | 33.3265 |

Table 8: Boat image sensitivity test in different position pixels.

| Pixels | (1, 1) | (27, 103) | (144, 178) | (201, 224) | (217, 105) | (255, 255) |
|---|---|---|---|---|---|---|
| NPCR (%) | 99.6120 | 99.5178 | 99.6349 | 99.6189 | 99.5735 | 99.4587 |
| UACI (%) | 33.4345 | 33.4383 | 33.4910 | 33.4351 | 33.4079 | 33.4939 |

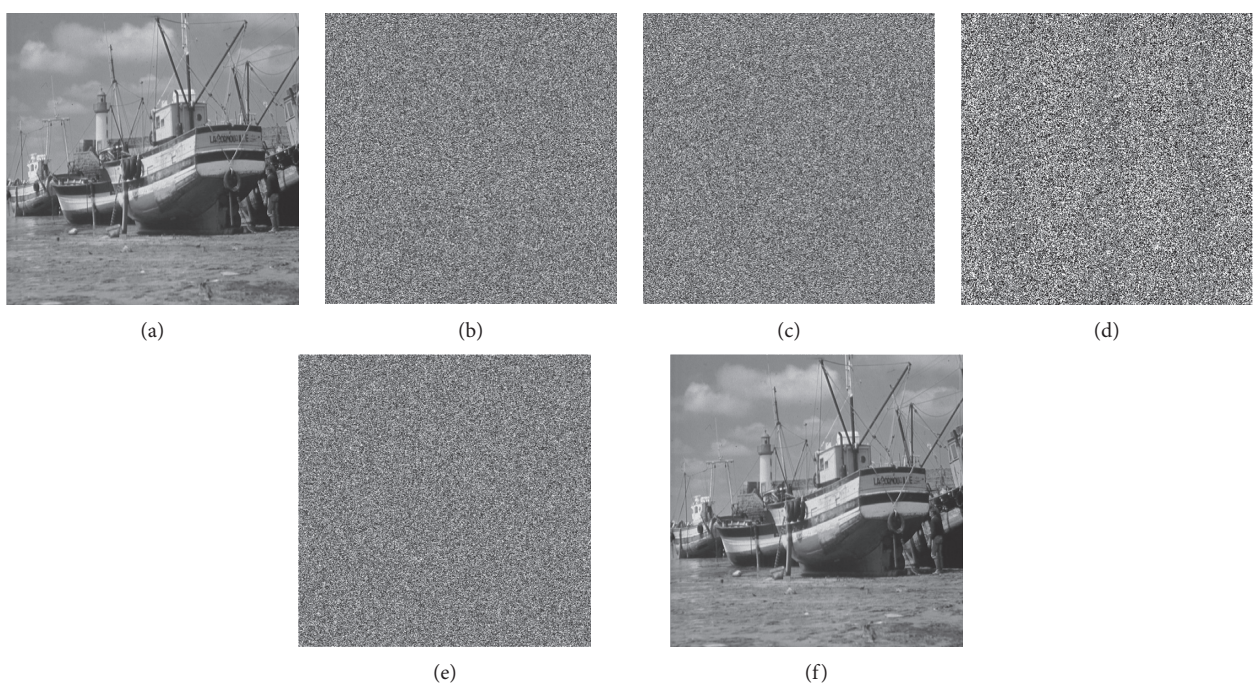

Figure 7: Key sensitivity analysis: (a) original image; (b) encrypted image using keys 1; (c) encrypted image using keys 2; (d) difference image of (b) and (c); (e) decrypted image using wrong keys 2; (f) decrypted image using correct key.

of Figures 7(b) and 7(c). When the wrong decryption key keys 2 is used to decrypt the image in Figure 7(b), the decryption result is obtained as shown in Figure 7(e). Figure 7(f) shows the correct decrypted image. The calculated NPCR and UACI values between the two encrypted images shown in Figures 7(b) and 7(c) were 99.60289% and

Table 9: Information entropy comparison with color Peppers images.

| Methods | R | G | B |
|---|---|---|---|
| Proposed method | 7.9993 | 7.9992 | 7.9993 |
| Ref. [54] | 7.9989 | 7.9991 | 7.9989 |
| Ref. [55] | 7.9971 | 7.9975 | 7.9974 |

33.43695%, respectively. This indicates that more than 99% of the pixels could be changed with just a single key change. It can be concluded that the proposed algorithm is highly sensitive to the key.

*6.6. Security Analysis.* Currently, two main methods are used to crack a password. One method involves an exhaustive search of the key. The cracking method attempts all possible key combinations. Because the RSA algorithm uses exponential calculations in both the encryption and decryption processes, its computational workload is huge, and deciphering using an exhaustive search is impossible. Therefore, cryptographic analysis is the only means of deciphering the encrypted information of the RSA algorithm. However, cracking RSA cryptography requires factorization of large integers. Although cracking low-order keys is possible, the factorization time increases exponentially with an increase in key length. As long as the length of $n$ meets certain requirements and appropriate parameters are selected, the algorithm based on RSA is safe.

*6.7. Comparison.* In this section, we make the comparison with color images by information entropy [54–56]. Table 9 shows the results. Therefore, the proposed method has good performance.

## 7. Conclusions

This study combined the Arnold map with the RSA public key encryption algorithm and proposed a new asymmetric image encryption scheme that considers the difficulty of large integer factorization to ensure its security. The initial parameters of the generalized Arnold map were generated by the RSA algorithm. Our study described the process whereby after the encryption operation by diffusion-confusion-diffusion is completed, the cipher image is formed from the plain image to achieve three layers of information hiding. The key used in the image encryption scheme is produced by the RSA algorithm to enhance the security of image transmission. Fortunately, the implementation process of this algorithm is simple and efficient. In addition, experimental results and tests show that the proposed asymmetric image encryption scheme is secure and effective and has high key sensitivity and good antiattack capabilities.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declare no conflict of interest.

## Acknowledgments

This work was supported in part by the National Natural Science Foundations of China (nos. 61702116 and 61972103), the Natural Science Foundation of Guangdong Province of China (no. 2019A1515011361), the Project of Enhancing School with Innovation of Guangdong Ocean University of China (no. Q18306), and the Postgraduate Education Innovation Project of Guangdong Ocean University of China (no. 202031).

## References

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

[2] P. Singh, A. K. Yadav, and K. Singh, "Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition," *Optics and Lasers in Engineering*, vol. 91, pp. 187–195, 2017.

[3] F. Yi, Y. Kim, and I. Moon, "Secure image-authentication schemes with hidden double random-phase encoding," *IEEE Access*, vol. 6, pp. 70113–70121, 2018.

[4] X. Huang and G. Ye, "An image encryption algorithm based on irregular wave representation," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2611–2628, 2018.

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

[6] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, vol. 29, no. 5, pp. 618–627, 2014.

[7] X. Lv, X. Liao, and B. Yang, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28633–28663, 2018.

[8] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[9] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 71–93, 2014.

[10] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm," *Optics and Lasers in Engineering*, vol. 121, pp. 169–180, 2019.

[11] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[12] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[13] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An image encryption scheme using lightweight bit-level confusion and

cascade cross circular diffusion," *Optics Communications*, vol. 285, no. 9, pp. 2343–2354, 2012.

[14] Z. Liu, L. Xu, T. Liu et al., "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp. 123–128, 2011.

[15] S. F. Raza and V. Satpute, "A novel bit permutation-based image encryption algorithm," *Nonlinear Dynamics*, vol. 95, no. 2, pp. 859–873, 2019.

[16] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Optics Letters*, vol. 31, no. 22, pp. 3261–3263, 2006.

[17] C. Wu, K.-Y. Hu, Y. Wang, J. Wang, and Q.-H. Wang, "Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 448, pp. 26–32, 2019.

[18] S. K. Rajput and N. K. Nishchal, "Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask," *Applied Optics*, vol. 51, no. 22, pp. 5377–5786, 2012.

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

[20] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[21] A. Sinha, "Nonlinear optical cryptosystem resistant to standard and hybrid attacks," *Optics and Lasers in Engineering*, vol. 81, pp. 79–86, 2016.

[22] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated fourier transforms," *Optics Letters*, vol. 35, no. 2, pp. 118–120, 2010.

[23] X. Deng and D. Zhao, "Single-channel color image encryption based on asymmetric cryptosystem," *Optics & Laser Technology*, vol. 44, no. 1, pp. 136–140, 2012.

[24] P. Rakheja, R. Vig, and P. Singh, "An asymmetric hybrid cryptosystem using hyperchaotic system and random decomposition in hybrid multi resolution wavelet domain," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 20809–20834, 2019.

[25] H. Chen, C. Tanougast, Z. Liu, and L. Sieler, "Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains," *Optics and Lasers in Engineering*, vol. 93, pp. 1–8, 2017.

[26] X. Wang and D. Zhao, "Double images encryption method with resistance against the specific attack based on an asymmetric algorithm," *Optics Express*, vol. 20, no. 11, pp. 11994–12003, 2012.

[27] T. Zhao, Q. Ran, and Y. Chi, "Image encryption based on nonlinear encryption system and public-key cryptography," *Optics Communications*, vol. 338, pp. 64–72, 2015.

[28] S. E. El-Khamy, N. O. Korany, and M. H. El-Sherif, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24091–24106, 2017.

[29] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95–105, 2018.

[30] F.-H. Hsiao, "Chaotic synchronization cryptosystems combined with RSA encryption algorithm," *Fuzzy Sets and Systems*, vol. 342, pp. 109–137, 2018.

[31] J.-x. Chen, Z.-l. Zhu, C. Fu, and H. Yu, "A fast image encryption scheme with a novel pixel swapping-based confusion approach," *Nonlinear Dynamics*, vol. 77, no. 4, pp. 1191–1207, 2014.

[32] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," *IETE Technical Review*, vol. 33, no. 3, pp. 310–322, 2016.

[33] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[34] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[35] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.

[36] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, Article ID 105816, 2020.

[37] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Optics and Lasers in Engineering*, vol. 124, p. 105821, 2020.

[38] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, "Optical image encryption technique based on compressed sensing and Arnold transformation," *Optik*, vol. 124, no. 24, pp. 6590–6593, 2013.

[39] X. Lv, X. Liao, and Y. Bo, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," *Multimedia Tools and Applications*, vol. 77, pp. 1–31, 2018.

[40] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[41] A. Belazi, H. Hermassi, R. Rhouma, and S. Belghith, "Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map," *Nonlinear Dynamics*, vol. 76, no. 4, pp. 1989–2004, 2014.

[42] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on DNA encoding and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7841–7869, 2019.

[43] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-based image encryption scheme," *Information Sciences*, vol. 520, pp. 130–141, 2020.

[44] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Processing: Image Communication*, vol. 52, pp. 6–19, 2017.

[45] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[46] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set," *Journal of Information Security and Applications*, vol. 50, p. 102428, 2020.

[47] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 2079–2087, 2012.

[48] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation

for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[49] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 51–66, 2017.

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

[51] K. A. K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-D chaotic maps," *Journal of Information Security and Applications*, vol. 46, pp. 23–41, 2019.

[52] X. Wang, Ü. Çavuşoğlu, S. Kacar et al., "S-box based image encryption application using a chaotic system without equilibrium," *Applied Sciences*, vol. 9, no. 4, p. 781, 2019.

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

[54] B. Y. Irani, P. Ayubi, F. A. Jabalkandi, M. Y. Valandar, and M. J. Barani, "Digital image scrambling based on a new one-dimensional coupled Sine map," *Nonlinear Dynamics*, vol. 97, pp. 2693–2721, 2019.

[55] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, Article ID 162921, 2019.

[56] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.