Mathematical Biosciences and Engineering

MBE, 18(5): 5427–5448.
DOI: 10.3934/mbe.2021275
Received: 06 May 2021
Accepted: 15 June 2021
Published: 18 June 2021

http://www.aimspress.com/journal/MBE

Research article

Asymmetric image encryption scheme based on the Quantum logistic map and cyclic modulo diffusion

Guodong Ye*, Huishan Wu, Kaixin Jiao and Duan Mei

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

* **Correspondence:** Email: guodongye@hotmail.com.

Abstract: In this study, a novel asymmetric image encryption scheme based on the Rivest-Shamir-Adleman (RSA) algorithm and Arnold transformation is proposed. First, the asymmetric public key RSA algorithm is used to generate the initial values for a quantum logistic map. Second, the parameters of the Arnold map are calculated. Then, Arnold scrambling operation is performed on the plain image to achieve the rough hiding of image information. Third, each row and each column of the image are taken as different units respectively and then exclusive-OR (XOR) diffusion is applied. Finally, the generated keystream is used to perform an end-to-start cyclic modulo diffusion operation for all rows and columns to produce the final cipher image. In addition, the keystream is related to the plain image, which can enhance the ability to resist chosen plaintext attack and known plaintext attack. The test results also show that the proposed encryption algorithm has strong plain sensitivity and key sensitivity.

Keywords: Quantum logistic map; Arnold map; image encryption; end-to-start cyclic modulo diffusion

1. Introduction

With rapid development of the Internet, information technology, and digital communications, the status of multimedia data transmission is increasing in modern society. Image is an important information carrier in human life to display or describe directly the objective phenomena. In recent years, owing to leakages of digital image information, serious consequences have occurred. Thus, image encryption protection has become particularly important. Traditional encryption algorithms

store and encrypt data as a one-dimensional string. As to images, due to the large amount of data, the calculation of encryption schemes is complicated, and the high correlation between the adjacent pixels requires a sufficient long keystream for a high security level. Therefore, a new encryption algorithm needs to be proposed for the secure communication of images.

A chaotic system refers to a deterministic system with seemingly random irregular movements, and its behavior is uncertain, unrepeatable, and unpredictable. Chaotic system is sensitive to initial conditions, and exhibits pseudorandom, ergodicity, and aperiodicity [1]. The combination of an image encryption algorithm and a chaotic system can effectively improve security and anti-cracking ability. Therefore, chaotic systems have been widely used in image encryption algorithms since they were proposed. For example, in [2], an algorithm with one-time-keys was proposed to resist brute-force attack. Albahrani et al. [3] designed a block method based image encryption with a cross map as a kind of chaotic map. To improve the robustness against common attacks, Yu et al. [4] proposed a new image encryption algorithm based on a short-time fractional Fourier transform (FrFT) and a hyperchaotic system. The diffusion operation and feedback system were designed to improve the anti-interference ability. Moreover, the use of the hyperchaotic system increases the key space and enhances sensitivity to all keys. In [5], a color image encryption algorithm was proposed by using a hyperchaotic system, of which can compress and encrypt an image according to the requirements of the reconstructed image quality. To hide efficiently the pixel distribution for the plain image, DNA based method was employed in [6] with the help of DNA random encoding rules. A generalized chaotic map and operation of fractional-order edge dection were applied into image encryption algorithm [7]. Besides of time domain encryption, Borujeni and Eshghi [8] suggested a hybrid domain based image encryption scheme including both frequency and time domains. Hybrid chaotic systems [9,10] were also be designed and applied for color image encryption Liu et al. [11] designed a new pathological image encryption scheme to ensure the secure transmission of pathological images in a telemedicine system. To effectively resist the plaintext attacks, Feng et al. [12] combined the discrete logarithm with a memristor-based chaotic system and proposed an image reconstruction encryption algorithm. The finite multiplication group used in this study has up to 128 generators, which can expand the key space and enhance the ability of the image encryption algorithm in resisting plaintext attacks. To compress multiple images into a small amount of data for the convenience of image transmission, Huang et al. [13] presented a nonlinear optical image encryption scheme that can encrypt images in both spatial and frequency domains, in which phase truncation and bitwise exclusive-OR (XOR) operation improve the robustness of the multi-image encryption scheme. In [14], a simple and efficient image encryption scheme was designed based on multiple piece-wise linear chaotic map systems. Rotational permutation operations and block diffusion operations were implemented to reach good encryption effect. Wang and Gao [15] studied the application of matrix semi-tensor product theory in a new chaotic image encryption with a Boolean network, scrambling, and diffusion. A new method of global pixel diffusion [16] by chaotic sequences was proposed for image encryption with a high security. In [17], a three-dimensional bit-level based image encryption algorithm was presented. Both the Rubik's cube method and the bit-level encryption principle were taken to realize scrambling operation. Some other image encryption algorithms [18–20] also show good performance by different hyeer-chaotic system, coupled map, and 2D chaotic map.

Arnold transformation is a common image pixel scrambling algorithm used to reduce the high correlation between pixels. Based on Arnold transformation and singular value decomposition (SVD)

in the fractional Hartley domain, a new phase image encryption scheme was proposed in [21]. Liu et al. [22] suggested a color image encryption algorithm using Arnold transformation and color mixing operation in the discrete cosine transform (DCT) domain. Arnold transformation was used to scramble the pixels of the three channels in color image, and the DCT was used to change the pixel values in the entire spatial distribution. Sui and Gao [23] proposed a color image encryption scheme using Gyrator transform and Arnold transformation, which has two security levels to protect image content. In the encryption and decryption processes, the rotation angle of the gyrator, number of iterations in Arnold transformation, parameters of the chaotic mapping, and generated accompanying phase function were all treated as the secret keys, thereby improving the security of the system. In [24], an optical color image encryption technique based on Arnold transformation and interferometry was proposed. Color image was decomposed into three channels R, G, B, and then each channel was encrypted into two random phase masks using Arnold transformation and interference method. Chen [25] used Arnold transformation to perturb the matrix pixels by encoding a single parameter, to form an image similar to color noise and to reduce the key space for storage and transmission applications. Wang et al. [26] suggested a fast algorithm for image encryption by parallel computing, in which parallelism of diffusion is designed to implement fast operation.

According to the classification of cryptosystems, cryptography can be divided into symmetric cryptography [27–30] and asymmetric (public key) cryptography [31–36]. In an asymmetric encryption algorithm, different keys are used for encrypting and decrypting, thereby realizing the nonlinearity of the algorithm, higher security, and convenient implementation of digital signature and verification. In [33], a scalable method of asymmetric image compression and encryption was proposed based on a discrete wavelet transform (DWT) and nonlinear operations in the cylindrical diffraction domain. DWT reduces the amount of data and is more conducive to data transmission. To enhance an encryption scheme with a larger key space than traditional cryptographic systems in the FT and FrFT fields, Ren et al. [37] designed an asymmetric image encryption scheme using a phase-truncated discrete multi-parameter FrFT. After a pixel scrambling and a random-phase mask, the asymmetric ciphertext with stable white noise was obtained through phase truncation.

In order to reduce the redundancy of image transmission, compression was also considered in image encryption. For example, Chai et al. [38] proposed a visually meaningful cipher image encryption by using technology of compressive sensing. Chaotic system, kronecker product, and singular value decomposition were all combined to produce the measurement matrix. In [39], a new chaotic color image encryption scheme was presented by multi-embedding strategy and compressive sensing. Each channel of R, G, and B were compressed to obtain measurements. Although there are many new image encryption algorithms have been published, some of them still have defects, for example, (i) The keystream is generated only dependent on the secret keys; (ii) It is hard to ensure the secure management of keys. In view of this, this paper combines quantum logistic map, Arnold transformation, and diffusion technology together with RSA to design an asymmetric encryption scheme, aiming to carry out high security, strong anti-attack and more suitable for network transmission. The innovations of this paper are: 1) Extract the text information of the plain image to be plain message. 2) Generate the cipher message by RSA and produce the initial conditions for quantum system by a new mathematical model. 3) Update the initial conditions by the text information of the plain image to enhance the plaintext dependence. 4) Build an end-to-start cyclic modulo diffusion operation.

The rest of this article is organized as follows. Section 2 briefly introduces the public key RSA

algorithm, Arnold transformation, and quantum logistic map. Section 3 gives the image encryption and decryption processes. Section 4 displays some experimental results. Section 5 discusses the various analytical tests of the encryption results. Section 6 presents the conclusions of this study.

2. Preparatory knowledges

2.1. RSA encryption algorithm

The public key RSA cryptosystem was proposed in 1978 by Rivest, Shamir, and Adleman. RSA encryption algorithm is an asymmetric encryption structure, which can complete the decryption operation without directly passing the keys. This method ensures security and avoids the risk of keys being cracked, which typically happens when keys are transmitted directly. In the whole encryption process, the key and algorithm are independently separated. Therefore, the key can be distributed more effectively. The specific description of the RSA algorithm is as follows:

Step 1: Randomly and secretly choose two large prime numbers p and q.

Step 2: Compute $n = p \times q$, $\varphi(n) = (p-1)(q-1)$, where $\varphi(n)$ is the Euler function of n.

Step 3: Randomly select e in range $1 < e < \varphi(n)$, satisfying $\gcd(e, \varphi(n)) = 1$, where e and $\varphi(n)$ are prime numbers.

Step 4: Calculate the decryption key d, where $e \times d = 1 \bmod(\varphi(n))$.

Step 5: Open integers n and e, and keep d in secret.

Step 6: Encrypt plaintext m to be ciphertext c by $c = m^e \bmod n$.

Step 7: Decrypt ciphertext c to be plaintext m by $m = c^d \bmod n$.

2.2. Quantum logistic map

Logistic map is a classical mathematical model used to study the behaviors of complex systems, such as dynamic systems, fractals, and chaos. In physics, if a physical quantity has the smallest indivisible basic unit, then this physical quantity is quantized, and the smallest unit is called a quantum. The quantum state is introduced into the chaotic system to form a quantum logistic map. The coupling of the system and harmonic oscillator path will produce a quantum logistic map with quantum correction. Akhshani et al. [40] applied quantum logistic map for image encryption, and its quantum logistic map is defined as,

$$\begin{cases} x_{n+1} = r(x_n - |x_n|^2) - r y_n \\ y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r[(2 - x_n - x_n^*) y_n - x_n z_n^* - x_n^* z_n] \\ z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r[2(1 - x_n^*) z_n - 2 x_n y_n - x_n \} \end{cases} \tag{1}$$

where β and r represent the dissipation parameter and adjustable parameter, respectively, and x_n^*, z_n^* are the conjugate complex numbers of x_n and z_n, respectively. When one sets $r = 3.99$ and $\beta \geq 6$, the quantum logistic map shows higher chaotic characteristics [40]. So, in this study, $r = 3.99$ and $\beta = 7$ are set with all initial parameters be real numbers. As pointed by [40]: classical nonlinear chaotic systems are famous because of their exponential sensitivity to each initial condition. However, the linearity of quantum mechanics not only shows such sensitivity to each initial condition, and also the Heisenberg uncertainty principle (HUP) prevents us from talking about initial conditions in quantum mechanics. Therefore, for this interesting property, quantum logistic map can

also be used in cryptography, for example image encryption. In view of these good characteristics of quantum logistic map, many image encryption algorithms [41–43] based on it have been proposed.

2.3. Arnold transformation

Arnold transformation is a scrambling operation that can randomly change the pixel position for an image, which is also called a cat map. By rearranging the pixels in a digital image matrix, the originally meaningful image will become a meaningless image. Arnold transformation is defined as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{2}$$

By replacing the matrix of above Arnold transformation, a generalized Arnold transformation can be obtained, which is defined as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{3}$$

where a,b and N are positive integers, (x_n, y_n) are the coordinates of the pixel in the original image, and (x_{n+1}, y_{n+1}) are the coordinate positions after transformation. Arnold transformation is a reversible mapping, and its corresponding inverse transformation is defined as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ab+1 & -b \\ -a & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{4}$$

Arnold transformation is reversible, and it is easy to be implemented. Therefore, this study combines Arnold transformation with the quantum logistic system and other technologies to design a new image encryption scheme.

3. The proposed image encryption scheme

3.1. Image encryption process

This study integrates the quantum logistic map, the RSA algorithm, the Arnold transformation, and the diffusion operation to realize a new asymmetric image encryption scheme. The framework of the proposed image encryption scheme is shown in Figure 1. The detail encryption steps are as follows:

Step 1: Select large prime numbers p and q, and calculate public key e and private key d.

Step 2: Read plain image P with size $M \times N$.

Step 3: Extract the text information of the image, i.e., $R = \sum_{i=1}^{M} \sum_{j=1}^{N} P(i, j)$, for public information.

Step 4: Select three plain parameters $a_i (i = 1, 2, 3)$ and encrypt them with the public key to

obtain the public parameters $c_i = a_i^e \bmod n$.

Step 5: Calculate the initial values: $x_0 = (c_1 + a_1)/(k_1c_1 + k_2a_1)$, $y_0 = (c_2 + a_2)/(k_1c_2 + k_2a_2)$, $z_0 = (c_3 + a_3)/(k_1c_3 + k_2a_3)$, where $k_1 = 3, k_2 = 5$.

Step 6: Update the initial values: $x_0' = \mathrm{mod}(x_0 + R_1, 1)$, $y_0' = \mathrm{mod}(y_0 + R_1, 1)$, $z_0' = \mathrm{mod}(z_0 + R_1, 1)$, where $R_1 = (R+1)/(255 \times M \times N + 1)$.

Step 7: The updated initial values are substituted into quantum logistic map. After discarding the first 500 values of the sequence, the chaotic sequences x, y, z are obtained.

Step 8: Process the sequences as,

$$\begin{cases} X = \mathrm{mod}(\mathit{fix}(x(1:M) \times 10^{14}), 256) \\ Y = \mathrm{mod}(\mathit{fix}(y(1:N) \times 10^{14}), 256) \\ Z = \mathrm{mod}(\mathit{fix}(z \times 10^{14}), 256) \end{cases} \tag{5}$$

Step 9: Perform Arnold scrambling operation on the plain image P to obtain the scrambled image A. The values of ma, mb, and mc in the Arnold map are calculated as

$$ma = \mathrm{mod}(sum(X), mc) + 1 \tag{6}$$

$$mb = \mathrm{mod}(sum(Y), mc) + 1 \tag{7}$$

where $mc = \mathrm{mod}(sum(Z), R) + 1$.

Step 10: For the image A, perform XOR diffusion operation by row for it to obtain image B as,

$$B_i = A_i \oplus X_i \tag{8}$$

where $i = 1, 2, \cdots, M$.

Step 11: Perform diffusion under modulo operation by row again to obtain image C as,

$$C_i = \mathrm{mod}(B_i + Z_i + C_{i-1}, 256) \tag{9}$$

where $i = 1, 2, \cdots, M$. C_0 is a constant.

Step 12: Connect the last row of image C with the first row of C and perform diffusion under modulo operation for rows again to obtain image D as,

$$D_1 = \mathrm{mod}(C_1 + Z_1 + C_M, 256) \tag{10}$$

$$D_i = \mathrm{mod}(C_i + Z_i + D_{i-1}, 256) \tag{11}$$

where $i = 2, 3, \cdots, M$.

Step 13: The column direction is similar to the row direction. For image D, take the column as a unit and perform the XOR diffusion operation on the corresponding component of each column and Y to obtain image E as,

$$E_j = D_j \oplus Y_j \tag{12}$$

where $j = 1, 2, \cdots, N$.

Step 14: Perform modulo diffusion to each column to obtain image F as,

$$F_j = \mathrm{mod}(E_j + Z_j + F_{j-1}, 256) \tag{13}$$

where $j = 1, 2, \cdots, N$. F_0 is a constant.

Step 15: Connect the last column of the image F with the first column of F and perform modulo diffusion in the column direction again to obtain the cipher image G as,

$$G_1 = \mathrm{mod}(F_1 + Z_1 + F_N, 256) \tag{14}$$

$$G_j = \mathrm{mod}(F_j + Z_j + G_{j-1}, 256) \tag{15}$$

where $j = 2, 3, \cdots, N$.

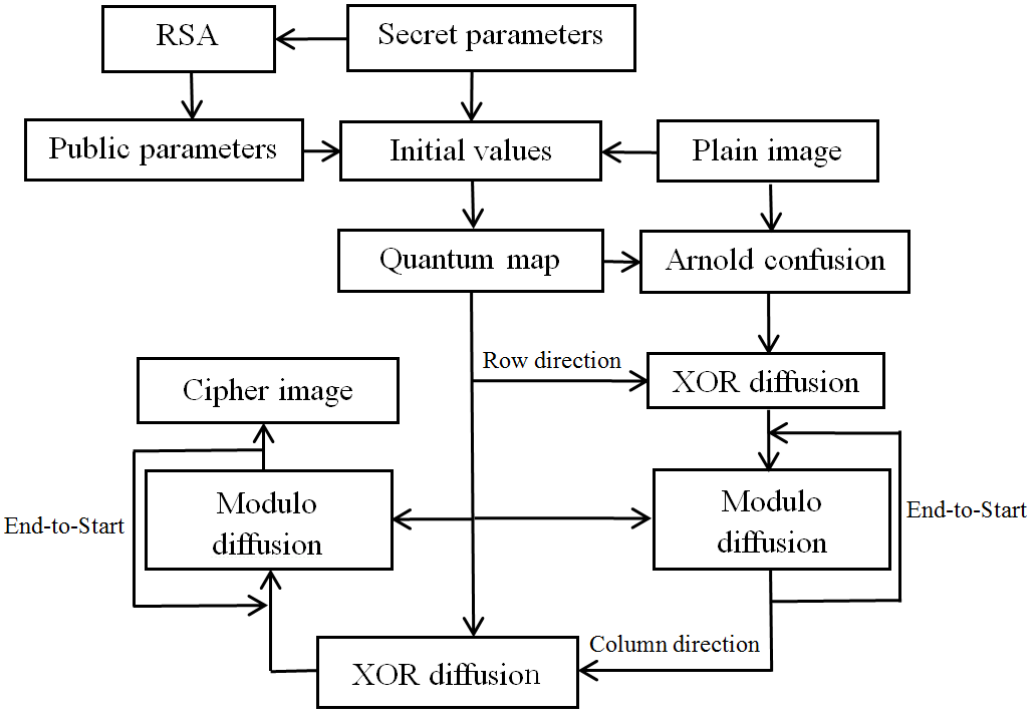


Figure 1. Flow of the proposed image encryption algorithm.

3.2. Image decryption process

The receiver has a cipher image G, public parameters c_1, c_2, c_3, r, β, and R, and private key (d, n). Figure 2 is the decryption flowchart of the proposed algorithm. The specific steps of decryption are as follows:

Step 1: Use the private key (d, n) to decrypt the public parameters $a_i = c_i^d \bmod n$.

Step 2: Read the cipher image G with size $M \times N$.

Step 3: Calculate the initial value $x_0 = (c_1 + a_1)/(3c_1 + 5a_1)$, $y_0 = (c_2 + a_2)/(3c_2 + 5a_2)$, $z_0 = (c_3 + a_3)/(3c_3 + 5a_3)$.

Step 4: Update the initial values $x_0' = \mathrm{mod}(x_0 + R_1, 1)$, $y_0' = \mathrm{mod}(y_0 + R_1, 1)$, $z_0' = \mathrm{mod}(z_0 + R_1, 1)$, where $R_1 = (R+1)/(255 \times M \times N + 1)$.

Step 5: By iterating quantum logistic map, and discarding the first 500 values of the sequence, obtain the chaotic sequence x', y', z'.

Step 6: Use Eq (5) to process the sequence and get X', Y', Z'.

Step 7: Calculate the two control parameters ma' and mb' of the Arnold map using Eqs (6) and (7).

Step 8: Use images G and Z' to perform the inverse modulo operation of the corresponding columns to derive image F' as,

$$F_j' = \mathrm{mod}(G_j - G_{j-1} - Z_j', 256) \tag{16}$$

$$F_1' = \mathrm{mod}(G_1 - Z_1' - F_N', 256) \tag{17}$$

where $j = 2,3,\cdots,N$.

Step 9: Use image F' to perform the inverse modulo operation of the corresponding columns to derive image E' as,

$$E_j' = \mathrm{mod}(F_j' - F_{j-1}' - Z_j', 256) \tag{18}$$

where $j = 1,2,\cdots,N$. F_0' is a constant.

Step 10: Use images E' and Y' to perform the XOR diffusion operation of the corresponding column to derive image D' as,

$$D_j' = E_j' \oplus Y_j' \tag{19}$$

where $j = 1,2,\cdots,N$

Step 11: The row direction is similar to the column direction. Use Z' to perform the inverse modulo diffusion operation in the row direction, and then use X' to perform the XOR diffusion of the corresponding rows to derive image A'.

Step 12: According to the parameter values ma' and mb', use Eq (4) to perform the inverse operation of the Arnold map and obtain the plain image P'.

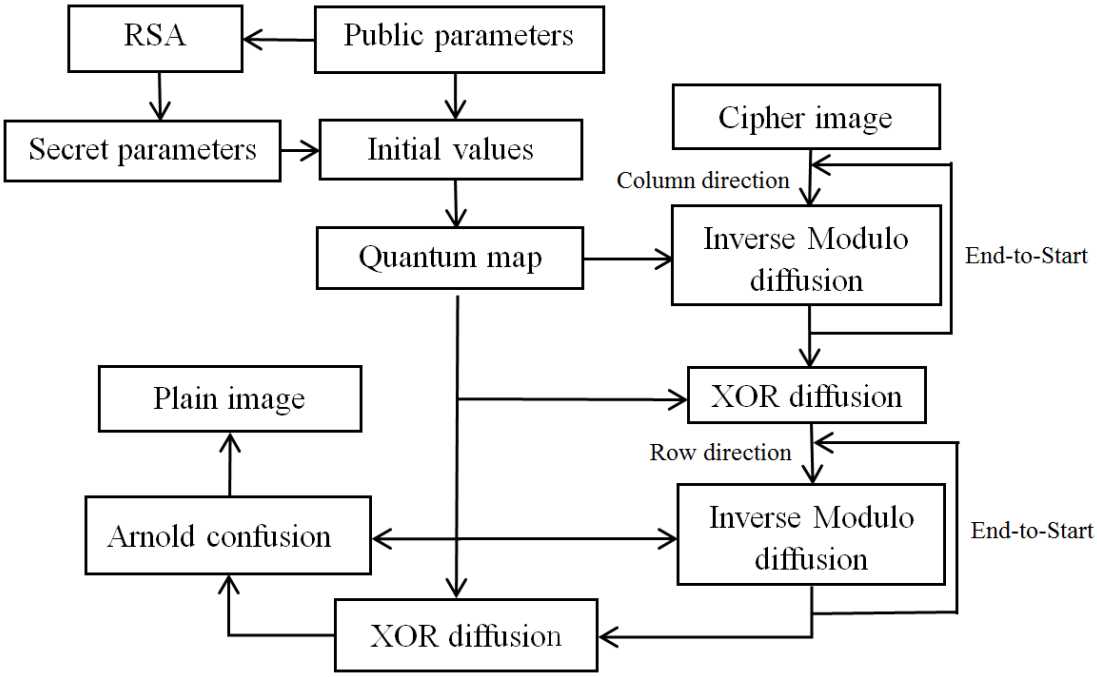


Figure 2. Flow of the proposed image decryption algorithm.

4. Experimental tests

Grayscale and color images (some from the USC-SIPI database) are taken for testing. Windows

10 operating system is used with an AMD Ryzen 7 1700 8-core processor and 8 GB memory, and the simulations are performed on MATLAB R2017b. Table 1 shows the values of each parameter in our test. Among them, a_1, a_2, a_3, q, p and d are the private keys, as well as e, r, β, c_1, c_2 and c_3 are the public keys. Figures 3 and 4 present the test images and their corresponding cipher images, respectively. So, no useful information about the plain image can be seen from these cipher images. Figure 5 shows the corresponding correct decrypted images. So, the proposed cryptographic scheme can be applied to both grayscale and color images. Table 2 shows the time required to encrypt images of different sizes. As we see that our scheme can be implemented by a fast way.

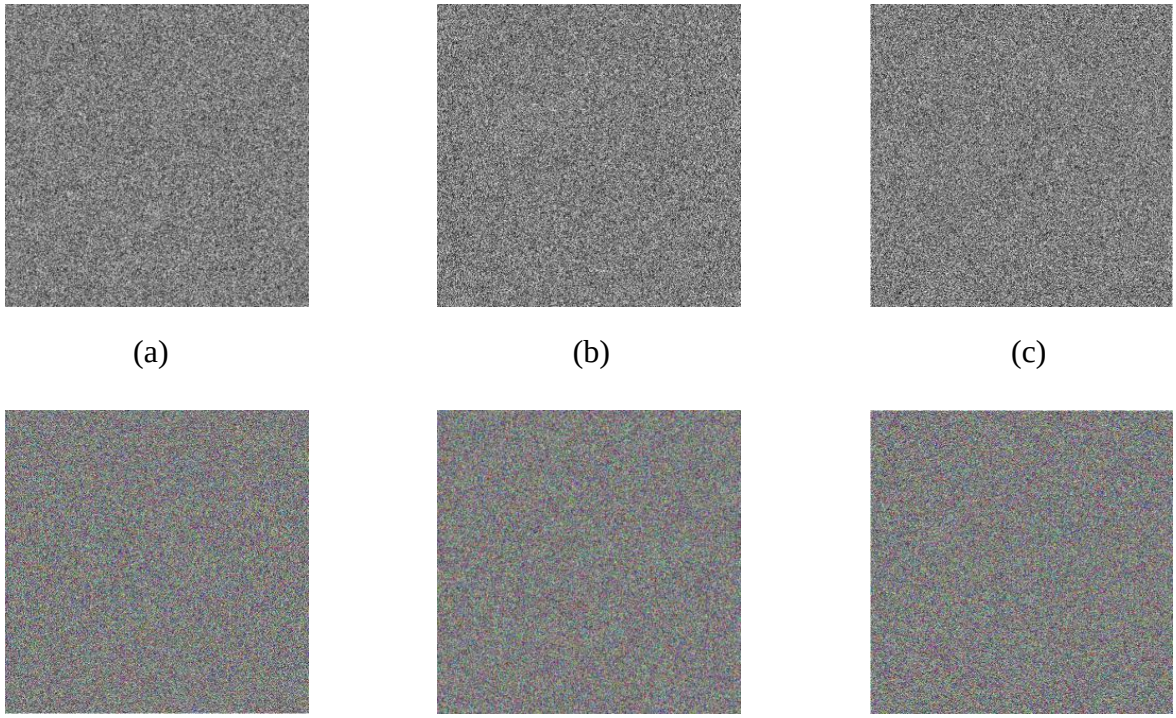
Table 1. Values of parameters in our experiment.

Parameter	Value	Parameter	Value
q	1733	a_2	15
p	1697	a_3	20
e	163	r	3.99
a_1	7	β	7
d	2,757,259	c_1	2,855,219
c_2	164,340	c_3	128,682

(a) (b) (c)

(d) (e) (f)

Figure 3. Plain images in grayscale: (a) Goldhill, (b) Sailboat, (c) Peppers; Cipher images in color: (d) Sun, (e) Baboon, (f) Peppers.



(a) (b) (c)

(d) (e) (f)

Figure 4. Cipher images for grayscale: (a) Goldhill, (b) Sailboat, (c) Peppers; Cipher images for color: (d) Sun, (e) Baboon, (f) Peppers.

(a) (b) (c)

(d) (e) (f)

Figure 5. Correct decrypted images for grayscale: (a) Goldhill, (b) Sailboat, (c) Peppers; Correct decrypted images for color: (d) Sun, (e) Baboon, (f) Peppers.

Table 2. Encryption time for different sizes (s).

Image size	Initial value generation	Confusion-diffusion encryption	Total time
256 × 256	0.014931	0.337695	0.394836
512 × 512	0.059334	0.699589	0.735226

5. Security analysis

5.1. Histogram analysis

Histogram analysis [44,45] shows how pixels are distributed in an image by plotting the number of observations for each brightness level. The frequency distribution of pixel values implies the statistical correlation between the plain images and the cipher images. A good image encryption system should have the ability to hide correlations; that is, the frequency distribution of the cipher on the pixel value is uniform, and the attacker cannot infer the plain information from it. To verify the uniformity of the pixel distribution of the proposed encryption algorithm, Figure 6 (a)–(c) and (d)–(f) show the histograms of the grayscale and encrypted images, respectively. Figure 7 is the histogram of the Baboon color image with three channels. To further evaluate the uniformity of the histogram, the statistical chi-square test was also performed, which is defined as,

$$\chi^2 = \sum_{L=0}^{255} \frac{(o_L - e_L)^2}{e_L} \tag{20}$$

where L is the intensity level, o_L and e_L are the observation reference and expected reference of the L gray level in the cipher image, respectively. The results of evaluating the uniformity of cipher images based on the chi-square values are shown in Table 3. Table 4 shows the chi-square comparison results. The smaller the chi-square value, the more uniform the pixel distribution and the higher the security. The histogram of the cipher image is evenly distributed, and the chi-square value is much smaller than the value of the plain image, which effectively improves resistivity against statistical attacks.

Table 3. Chi-square values of test images.

Image	Plain-image	Cipher-image	Results
Goldhill	161621.1816	279.9395	Pass
Sailboat	179772.6055	240.8535	Pass
Peppers (Grayscale)	138836.1738	287.2168	Pass
Sun	319180.5827	273.1582	Pass
Baboon	101863.4615	266.8301	Pass
Peppers (Color)	340999.4414	246.8555	Pass

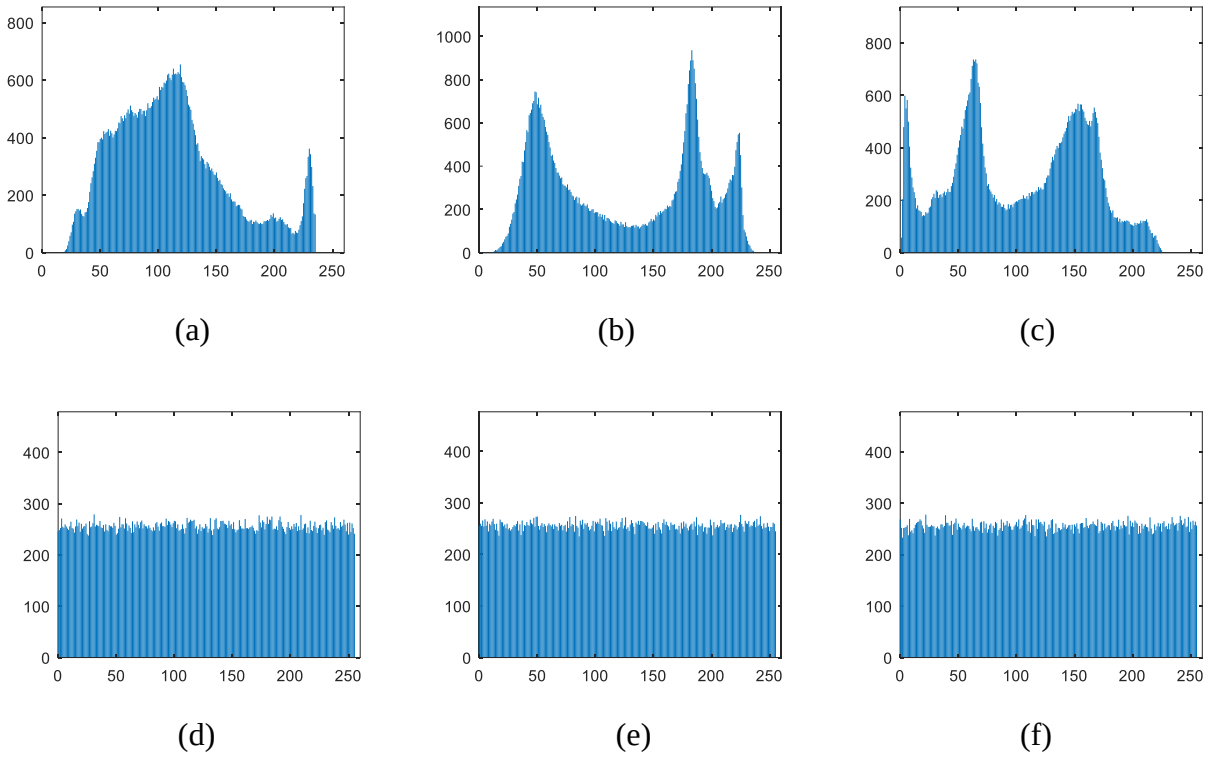


Figure 6. Histogram of the plain images: (a) Goldhill, (b) Sailboat, (c) Peppers. Histogram of the cipher images: (d) Goldhill, (e) Sailboat, (f) Peppers.

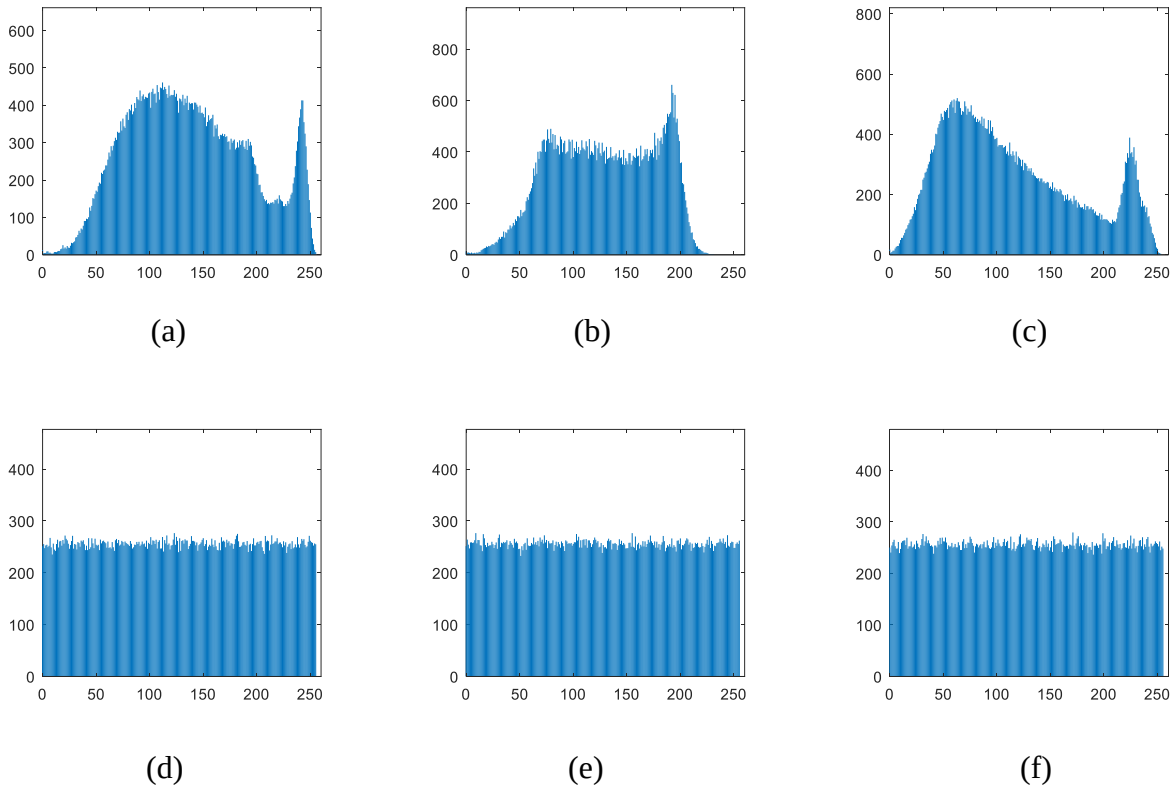


Figure 7. Histogram of the plain image Baboon: (a) R, (b) G, (c) B; Histogram of the cipher image Baboon: (d) R, (e) G, (f) B.

Table 4. Chi-square comparisons.

Reference	Baboon		
	R	G	B
This Paper	227.05	214.01	254.08
Ref. [46]	287.56	227.89	259.78

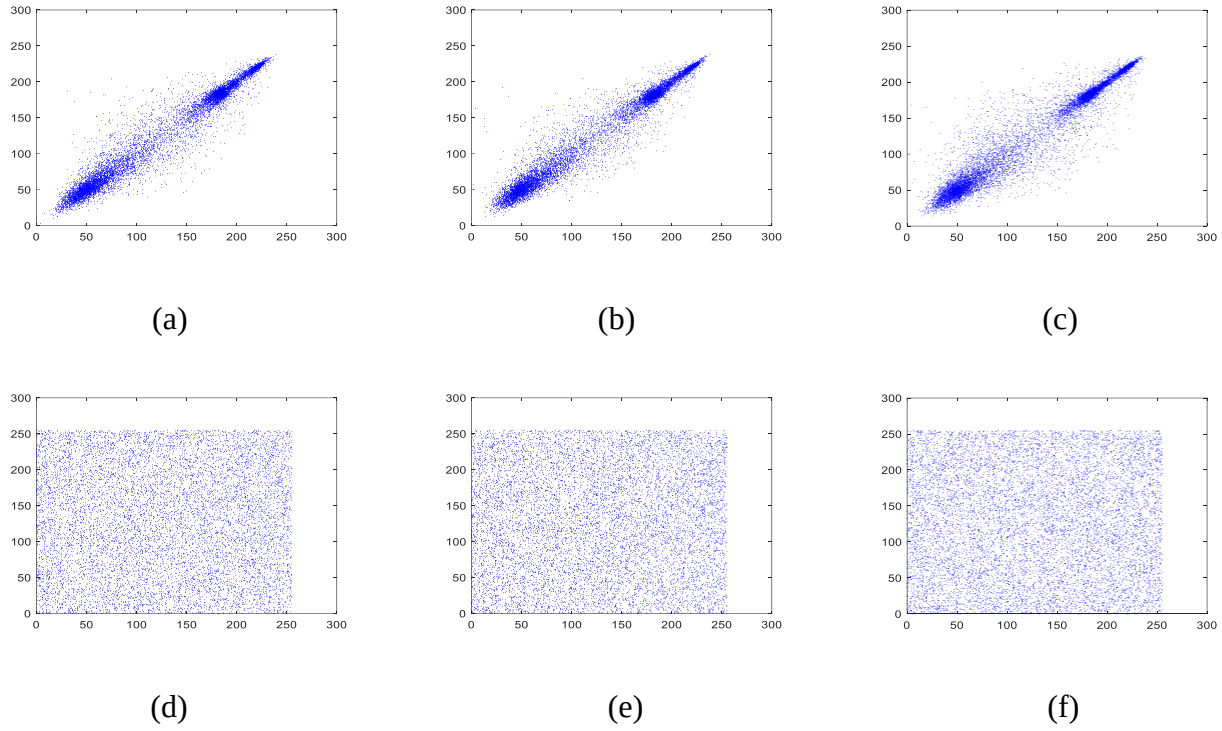


Figure 8. Correlation of the plain image sailboat: (a) horizontal direction, (b) vertical direction, (c) diagonal direction. Correlation of the cipher image sailboat: (d) horizontal direction, (e) vertical direction, (f) diagonal direction.

5.2. Correlation coefficient

Another measurement of statistical analyses is correlation [47–50]. For a natural digital image, there is a strong correlation between adjacent pixels in the horizontal, vertical, and diagonal directions. The lower correlation of adjacent pixels in a cipher image, the better performance of an encryption algorithm. A good cryptographic scheme should eliminate this correlation in a quantitative way to ensure security. The correlation coefficient is defined as

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

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

$$E(x') = \frac{1}{N}\sum_{i=1}^{N} x_i' \tag{23}$$

$$D(x') = \frac{1}{N}\sum_{i=1}^{N} (x_i' - E(x'))^2 \tag{24}$$

where $R_{x'y'}$ represents the correlation coefficient, x' and y' are the gray values of two adjacent pixels, and N is the total logarithm. Figure 8 shows the correlation of three directions of the grayscale image sailboat. Tables 5 and 6 show the correlation coefficient values of the test images. Table 7 shows the correlation coefficient comparisons of Baboon. The data in the tables show that the correlation coefficient of the plain images is close to 1, which means that the correlation coefficient between adjacent pixels is very strong. By using the proposed scheme, the values become close to 0, which means that our scheme can eliminate the strong correlation.

Table 5. Correlation coefficient tests for grayscale images.

Image	Plain-image			Cipher-image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Goldhill	0.9752	0.9708	0.9524	-0.0151	0.0209	0.0078
Sailboat	0.9721	0.9743	0.9602	0.0154	0.0106	0.0075
Peppers	0.9833	0.9796	0.9684	0.0139	0.0054	0.0153

Table 6. Correlation coefficients tests for color images.

Image	Direction	Plain-image			Cipher-image		
		R	G	B	R	G	B
Sun	Horizontal	0.9561	0.9504	0.9584	0.0049	-0.0041	0.0025
	Vertical	0.9553	0.9473	0.9569	0.0018	0.0102	0.0110
	Diagonal	0.9338	0.9258	0.9359	-0.0181	0.0029	-0.0087
Peppers	Horizontal	0.9660	0.9811	0.9661	0.0092	-0.0054	0.0103
	Vertical	0.9656	0.9822	0.9669	0.0059	0.0140	0.0118
	Diagonal	0.9584	0.9630	0.9489	-0.0093	0.0030	0.0092
Baboon	Horizontal	0.8620	0.7559	0.8838	-0.0033	0.0228	-0.0047
	Vertical	0.9230	0.8658	0.9104	0.0046	0.0063	-0.0045
	Diagonal	0.8536	0.7359	0.8428	0.0140	0.0050	0.0104

5.3. Information encryption

In information theory, entropy is an important index to measure the degree of randomness of a message. Ideally, each pixel of an 8-bit cipher image has a theory entropy value of 8. The higher the

information entropy value, the more uniform of gray value distribution and the more random of an image. The calculation formula of information entropy is,

$$H(x) = -\sum_{i=0}^{N} p(x_i) \log_2 p(x_i) \tag{25}$$

where $p(x_i)$ is the probability of the occurrence of x_i, and N is the total number of x_i. Tables 8 and 9 show the information entropy tests for different images. These results tell us that the information entropy values of the cipher image are very close to 8, indicating that the encryption scheme has strong randomness.

Table 7. Comparison of correlation coefficients of cipher image Peppers.

Method	Direction	Cipher-image		
		R	G	B
Ref. [49]	Horizontal	-0.0174	-0.0048	0.0086
	Vertical	-0.0021	-0.0020	0.0727
	Diagonal	0.0182	-0.0096	-0.0073
Ours	Horizontal	0.0092	-0.0054	0.0103
	Vertical	0.0059	0.0140	0.0118
	Diagonal	-0.0093	0.0030	0.0092

Table 8. Entropy test of grayscale images.

Image	Goldhill	Sailboat	Peppers
Plain-image	7.47778	7.48452	7.57148
Cipher-image	7.99923	7.99934	7.99921

Table 9. Entropy test of color images.

Image	Baboon			Peppers		
	R	G	B	R	G	B
Plain-image	7.70667	7.47443	7.75222	7.338832	7.496255	7.05831
Cipher-image	7.999377	7.99941	7.99927	7.99934	7.99924	7.99932

5.4. Local information encryption

Usually, an image has high data redundancy; therefore, its pixels have a high correlation with neighboring pixels. For a secure cipher image, the pixel values should be evenly distributed to achieve high randomness and high security. Local information entropy is another qualitative criterion for evaluating the randomness of an image, which is defined as,

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

where S_i represents the optional k groups of pixels in the image, and TB represents the number of pixels in S_i. The local information entropy values of the grayscale and color images are tested and shown in Tables 10 and 11, respectively. Based on these results, it can be seen that the local information entropy of the cipher image has surpassed 7.95, indicating that the distribution of pixel values inside the image is very uniform and random.

Table 10. Local information entropy of grayscale images.

Image	Goldhill	Sailboat	Peppers
Plain-local	6.48739	6.47318	6.55437
Cipher-local	7.95391	7.95486	7.95317

Table 11. Local information entropy of color images.

Image	Baboon			Peppers		
	R	G	B	R	G	B
Plain-local	6.75219	7.04211	7.00261	6.35622	6.45065	6.30729
Cipher-local	7.95617	7.95727	7.95342	7.95686	7.95521	7.95294

5.5. Differential attack analysis

The ideal property of a good encryption method should be sensitive to any small change in the plain image. That is, when the plain image has a small change in any pixel, the difference of the cipher image is analyzed to evaluate the diffusion performance of the encryption algorithm and should have the ability to resist differential attacks. The number of pixel change rate (NPCR) and unified average changing intensity (UACI) are two standards used for testing. The formulas are,

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j) \\ 1, & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \tag{27}$$

$$NPCR(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{D(i,j)}{M \times N} \times 100\% \tag{28}$$

$$UACI(C_1, C_2) = \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{M \times N \times 255} \times 100\% \tag{29}$$

where C_1 is one cipher image, C_2 is another cipher image with one pixel in the same plain image changes. The theory values for NPCR and UACI are 99.6093 and 33.4635% respectively. Tables 12 and 13 present the average values of NPCR and UACI for grayscale and color images, respectively.

Table 14 lists the comparisons by testing image Lena. All these test results show that the proposed asymmetric image encryption scheme has the ability to resist differential attacks.

Table 12. NPCR and UACI for grayscale images.

Image	NPCR	UACI
Goldhill	99.6124	33.4522
Sailboat	99.6129	33.4302
Peppers	99.6086	33.4398

Table 13. NPCR and UACI for color images.

Image	Sun			Baboon			Peppers		
	R	G	B	R	G	B	R	G	B
NPCR	99.6134	99.6107	99.5951	99.6089	99.5975	99.6017	99.6010	99.6126	99.6092
UACI	33.4784	33.4314	33.4631	33.4457	33.4622	33.4176	33.4744	33.4806	33.4139

Table 14. Comparisons of NPCR and UACI for image Lena.

Method	NPCR	UACI	Image size
Ours	99.6136	33.4643	512 × 512
Ours	99.6078	33.3123	256 × 256
Ref. [44]	99.7904	33.4970	512 × 512
Ref. [45]	99.6033	28.6797	512 × 512
Ref. [46]	99.5911	33.4208	256 × 256

5.6. Key sensitivity analysis

An extremely high key sensitivity can guarantee the security of an encryption system against the brute force attacks. To evaluate the sensitivity of keys, the 512×512 image Sailboat is used as an example for testing. Figure 9 shows the key sensitivity analysis results. Moreover, Figure 9(d) shows that even if a small key change occurs, the cipher image experiences a big difference. These test results show that only the correct key can decrypt the image, and the image encryption algorithm is highly sensitive to the keys and has the ability to resist brute force attacks.

5.7. Comparisons

The asymmetric image encryption algorithm proposed in this paper is suitable for grayscale and color images. Taking color image as an example, Table 15 shows the information entropy comparisons with other image encryption algorithms. The values in the table express that the information entropy result of the proposed scheme in this paper is closer to 8, indicating that the gray value distribution in the proposed asymmetric encryption scheme is more uniform and random than

that of other algorithms.

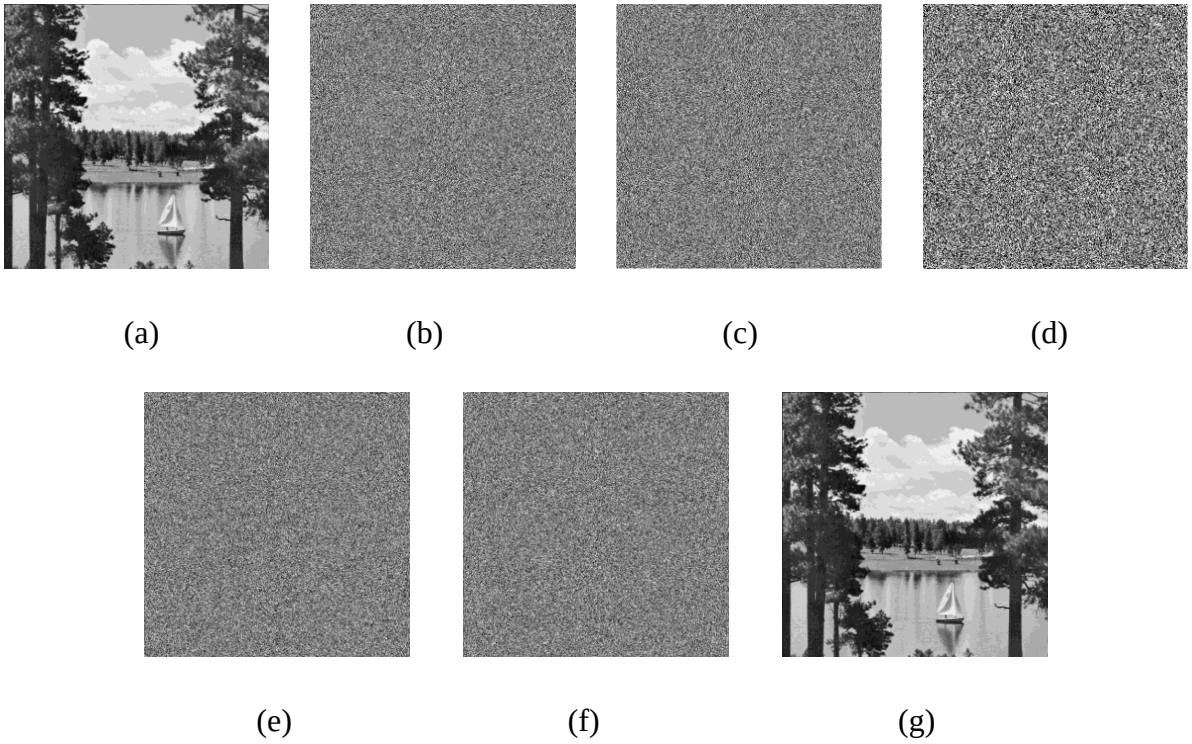


Figure 9. Key sensitivity test: (a) plain image; (b) cipher image; (c) cipher image with key $x_0 + 10^{-14}$; (d) difference of (b)-(c); (e) decrypted image using the keys of (c) for (b); (f) decrypted image using the keys of (b) for (c); (g) decrypted image with the correct key.

Table 15. Comparison among different schemes.

Image	size	Method	Information entropy		
			R	G	B
Peppers	512 × 512	Ours	7.9993	7.9992	7.9993
	256 × 256	Ours	7.9987	7.9984	7.9987
	256 × 256	Ref. [6]	7.9979	7.9979	7.9979
	512 × 512	Ref. [14]	7.9991	7.9992	7.9993
	256 × 256	Ref. [47]	7.9986	7.9987	7.9985
	256 × 256	Ref. [48]	7.9911	7.9912	7.9915
	256 × 256	Ref. [49]	7.9962	7.9929	7.9725
Baboon	512 × 512	Ours	7.9994	7.9994	7.9993
	256 × 256	Ours	7.9981	7.9982	7.9979
	256 × 256	Ref. [48]	7.9914	7.9915	7.9915
	256 × 256	Ref. [49]	7.9923	7.9803	7.9986

5.8. Conclusion and perspectives

This study employed a chaotic quantum logistic map, combining with both scrambling and diffusion operations, to propose a new asymmetric image encryption algorithm. First, the Arnold map was used to scramble the pixel positions of the plain images to achieve information hiding in the first layer. In the diffusion stage, different from the conventional point-to-point diffusion method, our solution took each row and each column as different units to perform diffusion operation. As to the row direction, the data in each row are first XOR-diffused. Then, each row in the image and the corresponding row in the keystream matrix are modulated and diffused; that is, two cyclic diffusions are realized by connecting the start and end. Operations to the column direction use a similar process to obtain the cipher image. Among them, the initial values of the quantum logistic map are related to the plain image, which can resist the known plaintext attack and chosen plaintext attack. Experimental tests and analyses show that the new asymmetric image encryption scheme proposed in this paper is suitable for both grayscale and color images, can better distribute pixel values be uniform, reduce high correlation, is highly sensitive to keys, and has the ability to resist various attacks.

However, there is still some disadvantages, for example, the compression operation was not considered in our scheme. So, in the future work, image can be compressed to reduce data redundancy, and how to achieve a good balance between the security and the complexity of image reconstruction should be taken into consideration. In addition, fast implement of encryption scheme is also an important issue in the future research.

Acknowledgments

The authors would like to thank the reviewers for their valuable comments and the editor's helpful suggestions. This work was supported in part by the National Natural Science Foundation of China (No.61972103), the Natural Science Foundation of Guangdong Province of China (No.2019A1515011361), and the Key Scientific Research Project of Education Department of Guangdong Province of China (No.2020ZDZX3064).

Conflict of interest

The authors declare that they have no conflict of interest.

References

1. G. D. Ye, K. X. Jiao, H. S. Wu, C. Pan, X. L. Huang, An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem, *Int. J. Bifurcat. Chaos*, **30** (2020), 2050233.
2. H. J Liu, Y. Q. Zhang, A. Kadir, Y. Q. Xu, Image encryption using complex hyper chaotic system by injecting impulse into parameters, *App. Math. Comput.*, **360** (2019), 83–93.
3. E. A. Albahrani, A. A. Maryoosh, S. H. Lafta, Block image encryption based on modified playfair and chaotic system, *J. Inf. Secur. Appl.*, **51** (2020), 102445.

4. S. S. Yu, N. R. Zhou, L. H. Gong, Z. Nie, Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system, *Opt. Laser Eng.*, **124** (2020), 105816.
5. X. J. Tong, M. Zhang, Z. Wang, J. Ma, A joint color image encryption and compression scheme based on hyper-chaotic system, *Nonlinear Dyn.*, **84** (2016), 2333–2356.
6. X. J. Kang, Z. H. Guo, A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system, *Signal Process. Image Commun.*, **80** (2020), 15670.
7. S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, M. F. Abu-ElYazeed, A novel image encryption system merging fractional-order edge detection and generalized chaotic maps, *Signal Process.*, **167** (2020), 107280.
8. S. E. Borujeni, M. Eshghi, Chaotic image encryption system using phase-magnitude transformation and pixel substitution, *Telecommun. Syst.*, **52** (2013), 525–537.
9. D. S. Malik, T. Shah, Color multiple image encryption scheme based on 3D-chaotic maps, *Math. Comput. Simulat.*, **178** (2020), 646–666.
10. M. Alawida, A. Samsudin, J. S. Teh, R. S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, *Signal Process.*, **160** (2019), 45–58.
11. H. J. Liu, A. Kadir, J. Liu, Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system, *Opt. Laser Eng.*, **122** (2019), 123–133.
12. W. Feng, Y. G. He, H. M. Li, C. L. Li, Image encryption algorithm based on discrete logarithm and memristive chaotic system, *Eur. Phys. J-Spec. Top.*, **228** (2019), 1951–1967.
13. Z. J. Huang, S. Cheng, L. H. Gong, N. R. Zhou, Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform, *Opt. Laser Eng.*, **124** (2020), 105821.
14. K. A. Patro, B. Acharya, An efficient colour image encryption scheme based on 1-D chaotic maps, *J. Inf. Secur. Appl.*, **46** (2019), 23–41.
15. X. Y. Wang, S. Gao, Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory, *Inf. Sci.*, **507** (2020), 16–36.
16. Y. J. Xian, X. Y. Wang, Fractal sorting matrix and its application on chaotic image encryption, *Inf. Sci.*, **547** (2021), 1154–1169.
17. H. G. Zhu, L.W. Dai, Y. T. Liu, L. J. Wu, A three-dimensional bit-level image encryption algorithm with Rubik' s cube method, *Math. Comput. Simulat.*, **185** (2021),754–770.
18. H. G. Zhu, X. D. Zhang, H. Yu, C. Zhao, Z. L. Zhu, An image encryption algorithm based on compound homogeneous hyper-chaotic system, *Nonlinear Dyn.*, **89** (2017), 61–79.
19. X. Y. Wang, J. J. Yang, A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient, *Inf. Sci.*, **569** (2021), 217–240.
20. H. G. Zhu, Y. R. Zhao, Y. J. Song, 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption, *IEEE Access*, **7** (2019), 14081–14098.
21. P. Singh, A. K. Yadav, K. Singh, Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition, *Opt. Laser Eng.*, **91** (2017),187–195.
22. Z. J. Liu, L. Xu, T. Liu, H. Chen, P. F. Li, C. Lin, et al., Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains, *Opt. Commun.*, **284** (2011), 123–128.
23. L. S. Sui, B. Gao, Color image encryption based on gyrator transform and Arnold transform, *Opt. Laser Technol.*, **48** (2013), 530–538.

24. W. Chen, C. Quan, C. J. Tay, Optical color image encryption based on Arnold transform and interference method, *Opt. Commun.*, **282** (2009), 3680–3685.
25. W. Chen, X. D. Chen, Optical image encryption using multilevel Arnold transform and noninterferometric imaging, *Opt. Eng.*, **50** (2011), 117001–117005.
26. X. Y. Wang, L. Feng, H Y Zhao, Fast image encryption algorithm based on parallel computing system, *Inf. Sci.*,**486** (2019), 340–358.
27. N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, Q. H. Liao, Quantum image encryption based on generalized Arnold transform and double random-phase encoding, *Quantum Inf. Process.*, **14** (2014), 1193–1213.
28. G. D. Ye, C. Pan, Y. X. Dong, K. X. Jiao, X. L. Huang, A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition, *Trans. Emerg. Telecommun. Technol.*, **32** (2021), e4071.
29. R. Ponuma, R. Amutha, Encryption of image data using compressive sensing and chaotic system, *Multimed. Tools Appl.*, **78** (2019), 11857–11881.
30. Y. X. Dong, X. L. Huang, G. D. Ye, Visually meaningful image encryption scheme based on DWT and schur decomposition, *Secur. Commun. Networks*, **2021** (2021), 6677325.
31. C. Wu, Y. Wang, Y. Chen, J. Wang, Q. H. Wang, Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain, *Opt. Commun.*, **413** (2019), 203–209.
32. W. Qin, X. Peng, Asymmetric cryptosystem based on phase-truncated fourier Transforms, *Opt. Lett.*, **35** (2010), 118–120.
33. C. Wu, K. Y. Hu, Y. Wang, J. Wang, Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain, *Opt. Commun.*, **448** (2019), 26–32.
34. J. H. Wu, X. F. Liao, B. Yang, Color image encryption based on chaotic systems and elliptic curve ElGamal scheme, *Signal Process.*, **141** (2017), 109–124.
35. G. D. Ye, K. X. Jiao, X. L. Huang, Quantum logistic image encryption algorithm based on SHA-3 and RSA, *Nonlinear Dyn.*, **104** (2021), 2807–2827.
36. S. K. Rajput, N. K. Nishchal, Image encryption based on interference that uses fractional Fourier domain asymmetric keys, *Appl. Opt.*, **51** (2012), 1446–1452.
37. G. H. Ren, J. N. Han, J. H. Fu, M. G. Shan, Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional Fourier transform, *Opt. Rev.*, **25** (2018), 701–707.
38. X. L. Chai, H. Y. Wu, Z. H. Gan, D. J. Han, Y. S. Zhang, Y. R. Chen, An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing, *Inf. Sci.*, **556** (2021), 305–340.
39. X. L. Chai, H. Y. Wu, Z. H. Gan, Y. S. Zhang, Y. R. Chen, Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy, *Signal Process.*, **171**(2020), 107525.
40. A. Akhshani, A. Akhavan, S. Lim, Z. Hassan, An image encryption scheme based on quantum logistic map, *Commun. Nonlinear Sci. Numer. Simul.*, **17** (2012), 4653–4661.
41. A. A. El-Latif, L. Li, N. Wang, Q. Han, X. M. Niu, A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, *Signal Process.*, **93** (2013), 2986–3000.
42. S. kuchaki, A novel color image encryption algorithm based on spatial permutation and quantum chaotic map, *Nonlinear Dyn.*, **81** (2015), 511–529.
43. J. Zhang, D. Huo, Image encryption algorithm based on quantum chaotic maps and DNA coding, *Multimed. Tools Appl.*, **78** (2019), 15605–15621.

44. Y. Q. Zhang, X. Y. Wang, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, *Inf. Sci.*, **273** (2014), 329–351.
45. X. Y. Wang, S. Gao, Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network, *Inf. Sci.*, **539** (2020), 195–214.
46. G. Z. Hu, B. B. Li, Coupling chaotic system based on unit transform and its applications in image encryption, *Signal Process.*, **178** (2021), 107790.
47. X. L. Chai, J. Q. Bi, Z. H. Gan, X. X. Liu, Y. S. Zhang, Y. R. Chen, Color image compression and encryption scheme based on compressive sensing and double random encryption strategy, *Signal Process.*, **176** (2020), 107684.
48. Y. Q. Zhang, Y. He, P. Li, X. Y. Wang, A new color image encryption scheme based on 2DNLCML system and genetic operations, *Opt. Laser Eng.*, **128** (2020), 106040.
49. X. Y. Wang, X. M. Qin, C. M. Liu, Color image encryption algorithm based on customized globally coupled map lattices, *Multimedia Tools Appl.*, **78** (2019), 6191–6209.
50. Z. H. Gan, X. L. Chai, M. H. Zhang, Y. Lu, A double color image encryption scheme based on three-dimensional brownian motion, *Multimedia Tools Appl.*, **77** (2018), 27919–27953.

AIMS Press