Hindawi
Journal of Applied Mathematics
Volume 2022, Article ID 9040702, 14 pages
https://doi.org/10.1155/2022/9040702

Research Article

A High-Security Privacy Image Encryption Algorithm Based on Chaos and Double Encryption Strategy

Zhiqiang Cheng,[1] Wencheng Wang,[2] Yuezhang Dai,[1] and Lun Li[2]

[1]*School of Physics and Electronic Information, Weifang University, Weifang 261061, China*
[2]*School of Mechanics and Automation, Weifang University, Weifang 261061, China*

Correspondence should be addressed to Lun Li; ll408907652@163.com

Received 29 May 2022; Revised 11 June 2022; Accepted 14 June 2022; Published 15 July 2022

Academic Editor: Tudor Barbu

Faces are widely used in information recognition and other fields. Due to the openness of the Internet, ensuring that face information is not stolen by criminals is a hot issue. The traditional encryption method only encrypts the whole area of the image and ignores some features of the face. This paper proposes a double-encrypted face image encryption algorithm. The contour features of the face are extracted, followed by two rounds of encryption. The first round of encryption algorithm encrypts the identified face image, and the second round of encryption algorithm encrypts the entire image. The encryption algorithm used is scrambling and diffusion at the same time, and the keystream of the cryptosystem is generated by 2D SF-SIMM. The design structure of this cryptosystem increases security, and the attacker needs to crack two rounds of the algorithm to get the original face image.

1. Introduction

Nowadays, in the era of rapid development of the Internet, people can receive and publish information through the Internet anytime, anywhere. Images are the most intuitive carrier for obtaining information. Nowadays, images have been widely used in military, medical, and other fields. As an important information-sharing carrier, image is a hot issue in realizing image security sharing and transmission [1–5]. Image encryption technology is one of the important technologies for image protection. Image encryption technology can convert a regular plaintext image into an unrecognizable noise image [6–9].

Traditional encryption schemes such as AES are not suitable for digital images, which makes image encryption algorithms based on chaos theory gradually favored by researchers. There is a common connection between the pseudorandom keystream generated by chaos and cryptography, which makes image encryption algorithms based on chaos theory widely used [10–13]. At the same time, the current research on chaos theory is also deepening. The combination of chaos theory and other technologies increases the complexity of the cryptographic system, making the proposed cryptographic system more secure [14–18].

For example, the DNA encryption algorithm based on chaos [19–21]: Yang et al. proposed CGI image encryption, which uses logistic chaotic to generate the keystream of the cryptosystem and combines with DNA encoding to obtain ciphertext images. This method reduces the number of key transmissions and has great advantages in image encryption with large amounts of data [19]. Quantum encryption algorithm based on chaos theory [22–24]: the keystream generated by the four-wing chaotic system is XORed with the plaintext to obtain a semiencrypted ciphertext image, and quantum rotation is used to complete the encryption operation in the diffusion stage. The experimental results are good, but the time of this algorithm is very slow [22]. In Ref. [25], compressed sensing and chaos theory are used to encrypt images, which reduces the amount of information transmission and increases the complexity of the algorithm, but the encryption process is lossy.

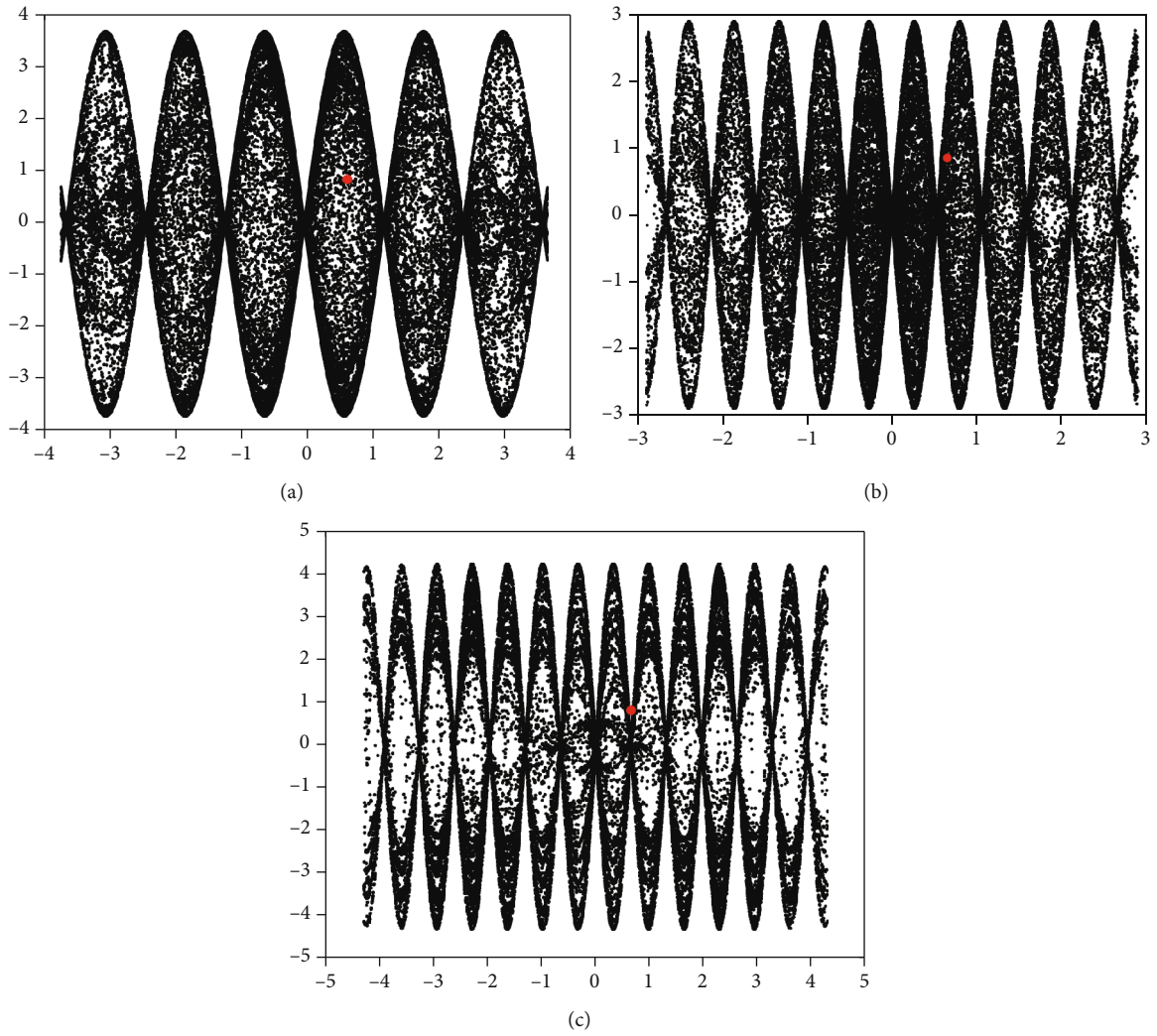


Figure 1: Trajectory diagram of 2D SF-SIMM. (a) Trajectory diagram with $\eta = 3.7$, $\theta = 5.2$, and $\lambda = 2.6$. (b) Trajectory diagram with $\eta = 2.9$, $\theta = 6.8$, and $\lambda = 5.9$. (c) Trajectory diagram with $\eta = 4.3$, $\theta = 2.2$, and $\lambda = 4.8$.

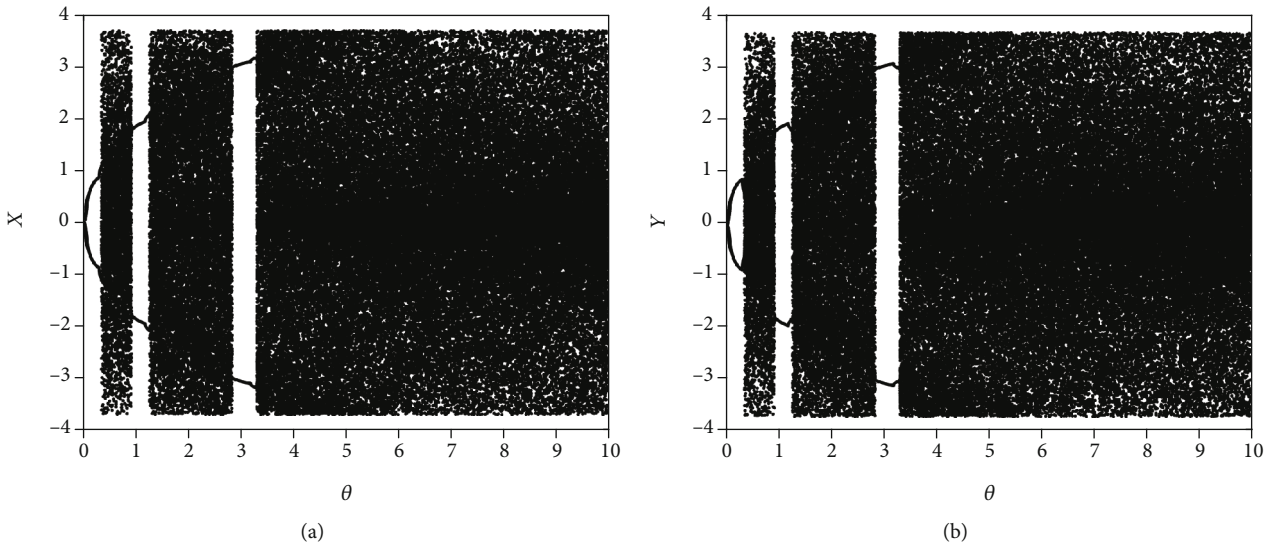
As one of the most private images in images, face images have been used in the field of information recognition, such as unlocking mobile phones. Ensuring more secure transmission of face images on the Internet is one of the most important topics in cryptography today. The above-mentioned image encryption algorithms are global encryption of the image. In this paper, we propose a double-encrypted image encryption algorithm for face images. The outline of the face is identified for the first encryption, followed by the second encryption of the entire image. Compared with traditional encryption algorithms, the proposed algorithm has higher security. An attacker needs to crack two rounds of the encryption algorithm to get the original face image. Compared with cracking the algorithm once, there is no doubt that it takes more time to crack the encryption algorithm twice. Furthermore, to improve the security of the encryption system, we use a strategy of simultaneous diffusion and scrambling, which has a higher complexity. In the designed cryptosystem, the required keystream is generated by 2D SF-SIMM. The 2D SF-SIMM [26] was proposed by Liu et al.; this system has three control parameters and more complex dynamic behavior. Therefore, the cryptosystem based on 2D SF-SIMM has a large key space.

2. Related Works

2.1. 2D SF-SIMM. The 2D SF-SIMM was proposed by Liu et al. It is a system composed of four sins and has three control parameters. Compared with other 2D chaotic systems, 2D SF-SIMM has a larger parameter space and better performance. It is described as

$$\begin{cases} f_{n+1} = \eta \sin(\lambda g_n) \sin(\theta / f_n) \\ g_{n+1} = \eta \sin(\lambda f_{n+1}) \sin(\theta / g_n) \end{cases}, \quad (1)$$

where η, θ, and λ are the three control parameters of the 2D SF-SIMM, $\eta \in (-\infty, +\infty)$, $\theta \in (-\infty, +\infty)$, and $\lambda \in (-\infty, +\infty)$. When $\eta\lambda > 1$, at that time, the system exhibits strong chaotic behavior. The trajectory diagram of the 2D SF-



(a) (b)

Figure 2: Bifurcation diagram of 2D SF-SIMM. (a) Bifurcation diagram of sequence X with $\eta = 3.7$ and $\lambda = 2.6$. (b) Bifurcation diagram of sequence Y with $\eta = 3.7$ and $\lambda = 2.6$.

(a) (b)

(c) (d)

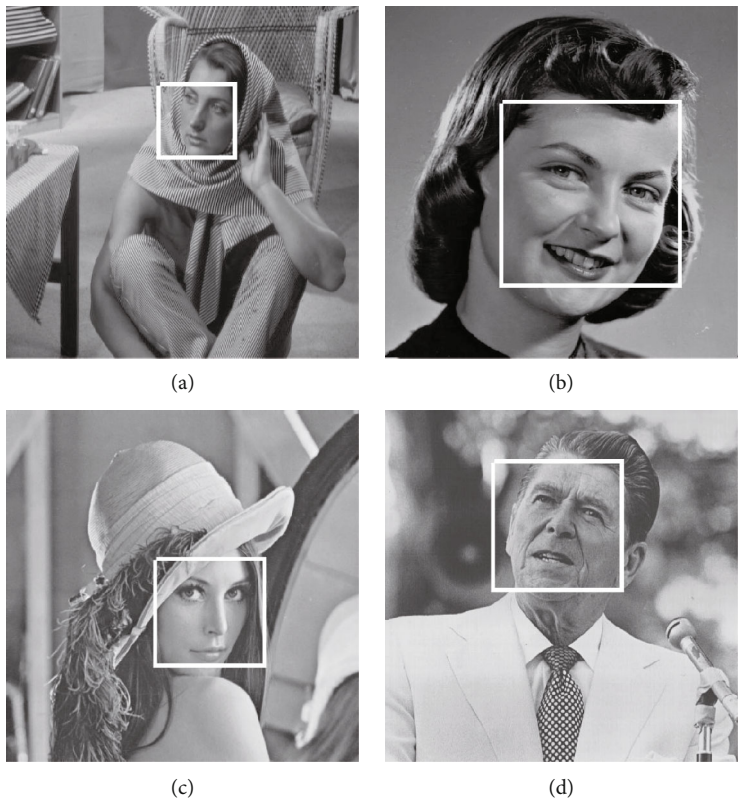
Figure 3: Face contour of face images. (a) Barbara. (b) Girl. (c) Lena. (d) Reagan.

SIMM is shown in Figure 1. The selected initial values are $x_0 = 0.65478466897887$ and $y_0 = 0.85426984531656$. The bifurcation diagram of the 2D SF-SIMM is shown in Figure 2. The selected initial values are $x_0 = 0.52169852522365$ and $y_0 = 0.96655412365898$.

2.2. Extraction of Facial Contours. The open source OpenCV is used to realize the detection of face contours. In this paper, the image data is used as shown in Figure 3. The face image extracted using OpenCV is shown in Figure 4.

3. Face Encryption Algorithm

The proposed encryption algorithm is a double encryption algorithm; the first is the encryption of the extracted face, and the second is the encryption of the whole image. In



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

Figure 4: Visualization for Barbara. (a) First encryption. (b) Second encryption. (c) Decrypt for the first time. (d) Decrypt for the second time.

the encryption algorithm, a strategy of scrambling and diffusion is proposed at the same time. This approach has been shown to have high complexity. In addition, this algorithm is a symmetric encryption algorithm, and the encryption process is the reverse process of decryption.

3.1. The Encryption Algorithm. The encryption algorithm is described as follows.

Input: P (P is a plaintext image)

Step 1: according to the plaintext P, generate an initial revision key k

$$k = \frac{1}{m_1 \times n_1} \sum_{i=1}^{m_1} \sum_{j=1}^{n_1} P(i,j), \tag{2}$$

where $m_1 = \text{size}(P, 1)$ and $n_1 = \text{size}(P, 2)$.

Step 2: bring k into the logistic iteration for 100 times to generate a new revision key k_1

$$f_{n+1} = \left(3.999 + \frac{k1}{10000}\right) \times f_n \times (1 - f_n), \tag{3}$$

where $n = 1, 2, 3, \cdots, 100$, $f_1 = k$, and $k_1 = f_{100}$.

Step 3: given the initial keys $x_0, y_0, \eta, \theta, \lambda$, generate the key of the cryptosystem by Equation (4) according to the revised key k_1

Input: X and N
$Y = X(1 : N)$
$YM = 1, 2, 3, 4, \cdots, M$
$YM2 = [Y ; YM]$
$YM3 = \text{sortrows}(YM2, 1)$
$s = YM3(1 : \text{end}, 2)$
Output: s

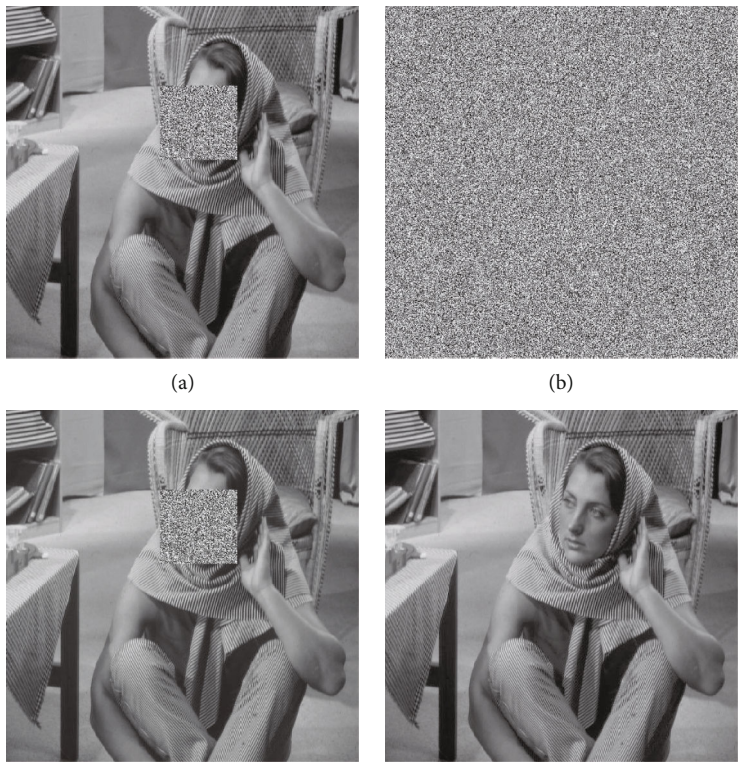
Algorithm 1: $(s = S(X, N))$.

$$\begin{cases} x_0 = x_0 + k_1, \\ y_0 = y_0 + k_1, \\ \eta = \eta + k_1, \\ \theta = \theta + k_1, \\ \lambda = \lambda + k_1. \end{cases} \tag{4}$$

Step 4: the new keys $x_0, y_0, \eta, \theta, \lambda$ are brought into the 2D SF-SIMM to generate the keystream of the cryptosystem X and Y

$$\begin{cases} x_{n+1} = \eta \sin(\lambda y_n) \sin\left(\dfrac{\theta}{x_n}\right), \\ y_{n+1} = \eta \sin(\lambda x_{n+1}) \sin\left(\dfrac{\theta}{y_n}\right), \end{cases} \tag{5}$$

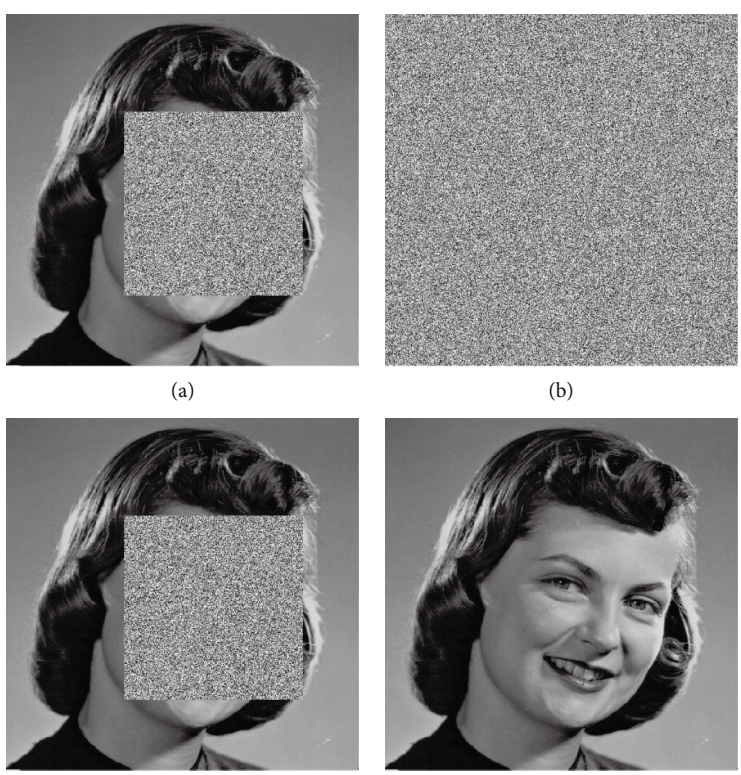
where the size of X is $m_1 \times n_1$ and the size of Y is $m_1 \times n_1$.



(a) (b)

(c) (d)

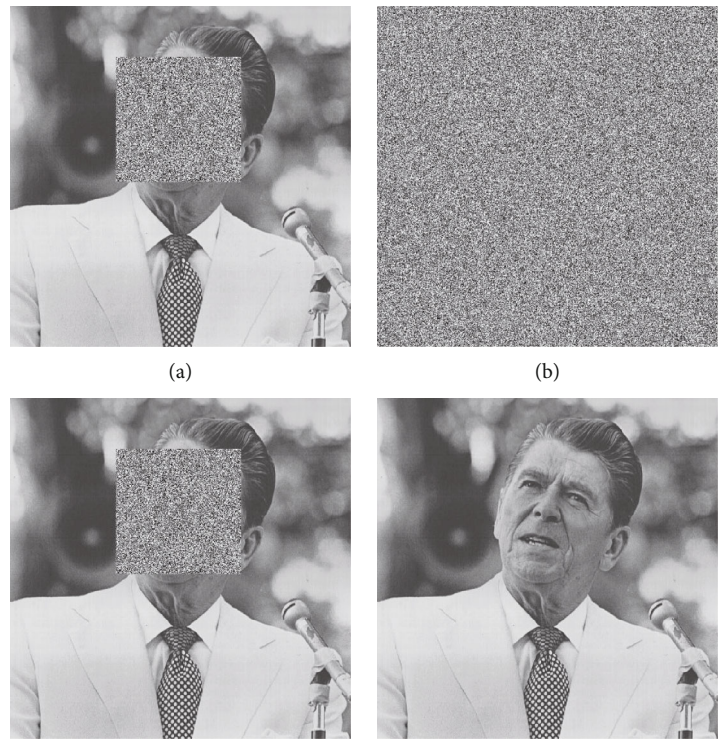
Figure 5: Visualization for Barbara. (a) First encryption. (b) Second encryption. (c) Decrypt for the first time. (d) Decrypt for the second time.



(a) (b)

(c) (d)

Figure 6: Visualization for girl. (a) First encryption. (b) Second encryption. (c) Decrypt for the first time. (d) Decrypt for the second time.



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

Figure 7: Visualization for Reagan. (a) First encryption. (b) Second encryption. (c) Decrypt for the first time. (d) Decrypt for the second time.

Step 5: extract the face contour, where the contour coordinates are $A = (a_1, a_2, a_3, a_4)$, a new plaintext is generated $F = P(a_1 : a_2, a_3 : a_4)$, $m_2 = \text{size}(F, 1)$, and $n_2 = \text{size}(F, 2)$.

Step 6: generate three sorting matrices S_1, S_2, S_3 for encryption stage by Algorithm 1.

$$\begin{cases} S_1 = S(X, m_1 \times n_1), \\ S_2 = S(Y, m_2 \times n_2), \\ S_3 = S(Y, m_1 \times n_1). \end{cases} \tag{6}$$

Step 7: three encryption matrices D_1, D_2, D_3 are generated for the encryption stage

$$\begin{cases} D_1 = \text{mod}\left(\text{floor}\left(X[1 : m_1 \times n_1] \times 10^{12}\right), 256\right), \\ D_2 = \text{mod}\left(\text{floor}\left(Y[1 : m_2 \times n_2] \times 10^{13}\right), 256\right), \\ D_3 = \text{mod}\left(\text{floor}\left(Y[1 : m_1 \times n_1] \times 10^{14}\right), 256\right). \end{cases} \tag{7}$$

Step 8: the first encryption, encrypting the extracted face image,

$$\begin{aligned} C_1[S_2(1)] &= F[S_2(1)] + D_2[S_2(1)] \bmod 256, \\ C_1[S2(i)] &= F[S2(i)] + D_2[S2(i)] + C_1[S2(i-1)] \\ &\quad \cdot \bmod 256, \quad i = 1, 2, 3, \cdots, m_2 \times n_2. \end{aligned} \tag{8}$$

Table 1: NIST test of plaintext and ciphertext.

Statistical test	Plaintext		Ciphertext	
	P value	Result	P value	Result
Nonoverlapping template matching	0	No	0.9797	Yes
Runs	0	No	0.4389	Yes
Serial	0	No	0.1111	Yes
Spectral	0	No	0.2581	Yes
Rank	0	No	0.4087	Yes
Random excursions	0	No	0.5949	Yes
Cumulative sums	0	No	0.2622	Yes
Frequency	0	No	0.6028	Yes
Universal	0	No	0.7112	Yes
Linear complexity	0	No	0.2217	Yes
Longest run of ones	0	No	0.1174	Yes
Approximate entropy	0	No	0.2967	Yes
Random excursion variant	0	No	0.3188	Yes
Block frequency	0	No	0.4242	Yes
Overlapping template matching	0	No	0.5079	Yes

Combine the new ciphertext with the original plaintext to produce a new plaintext image $P(a_1 : a_2, a_3 : a_4) = C_1$.

Step 9: the second encryption is to encrypt the entire image. This encryption is divided into backward encryption and forward encryption.

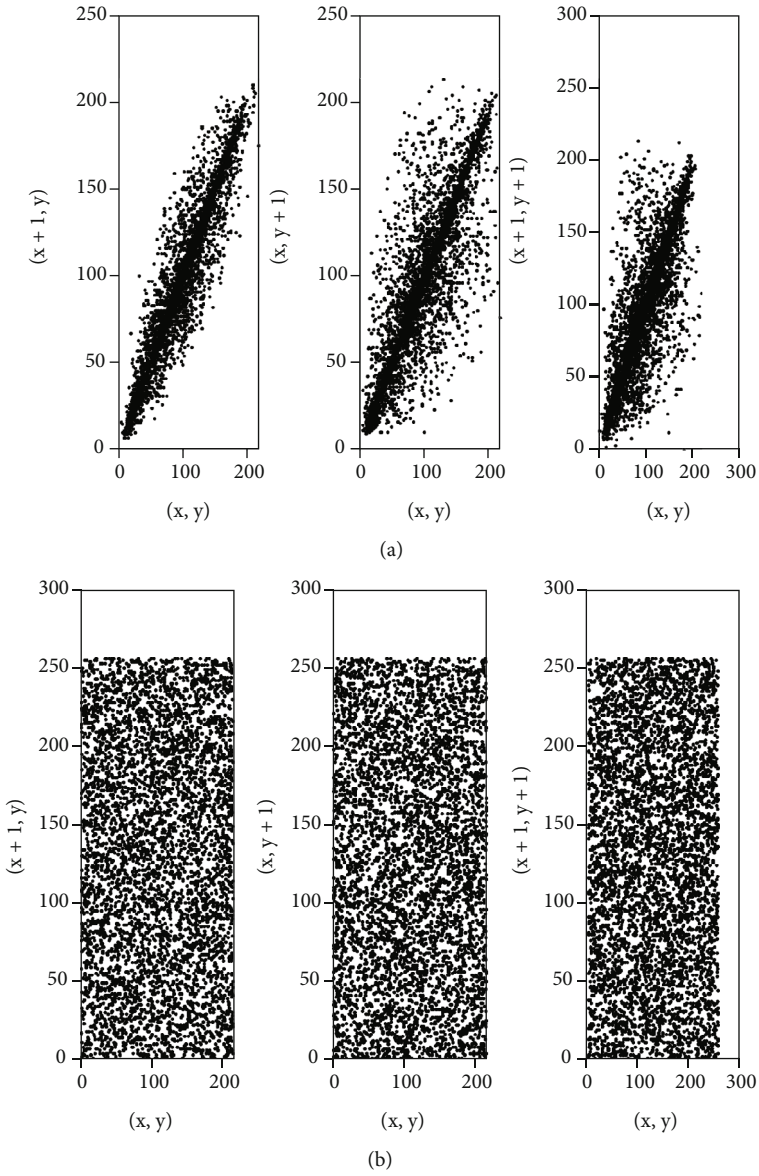


Figure 8: Correlation analysis of Barbara. (a) Correlation analysis of plaintext. (b) Correlation analysis of ciphertext.

Backward encryption is described as

$$\begin{aligned} C_2[S_1(1)] &= P[S_1(1)] + D_1[S_1(1)] \bmod 256, \\ C_2[S_1(i)] &= P[S_1(i)] + D_1[S_1(i)] + C_2[S_1(i-1)] \\ &\quad \cdot \bmod 256, \quad i = 1, 2, 3, \cdots, m_1 \times n_1. \end{aligned} \tag{9}$$

Forward encryption is described as

$$\begin{aligned} C_3[S_3(m_1 \times n_1)] &= C_2[S_3(m_1 \times n_1)] + D_3[S_3(m_1 \times n_1)] \\ &\quad \cdot \bmod 256, \\ C_3[S_3(i)] &= C_2[S_3(i)] + D_3[S_3(i)] + C_3[S_3(i+1)] \\ &\quad \cdot \bmod 256, \quad i = m_1 \times n_1 - 1, m_1 \times n_1 - 2, \cdots, 1. \end{aligned} \tag{10}$$

Output: C_3.

3.2. The Decryption Algorithm. The decryption algorithm is described as follows.

Input: C_3 (C_3 is the ciphertext image), secret keys are $x_0, y_0, \eta, \theta, \lambda$, and k_1.

Step 1: given the initial key $x_0, y_0, \eta, \theta, \lambda$, generate the key of the cryptosystem based on the revised key k_1

$$\begin{cases} x_0 = x_0 + k_1, \\ y_0 = y_0 + k_1, \\ \eta = \eta + k_1, \\ \theta = \theta + k_1, \\ \lambda = \lambda + k_1. \end{cases} \tag{11}$$

Step 2: the keystream of the cryptosystem D_1, D_2, D_3 and S_1, S_2, S_3 are generated.

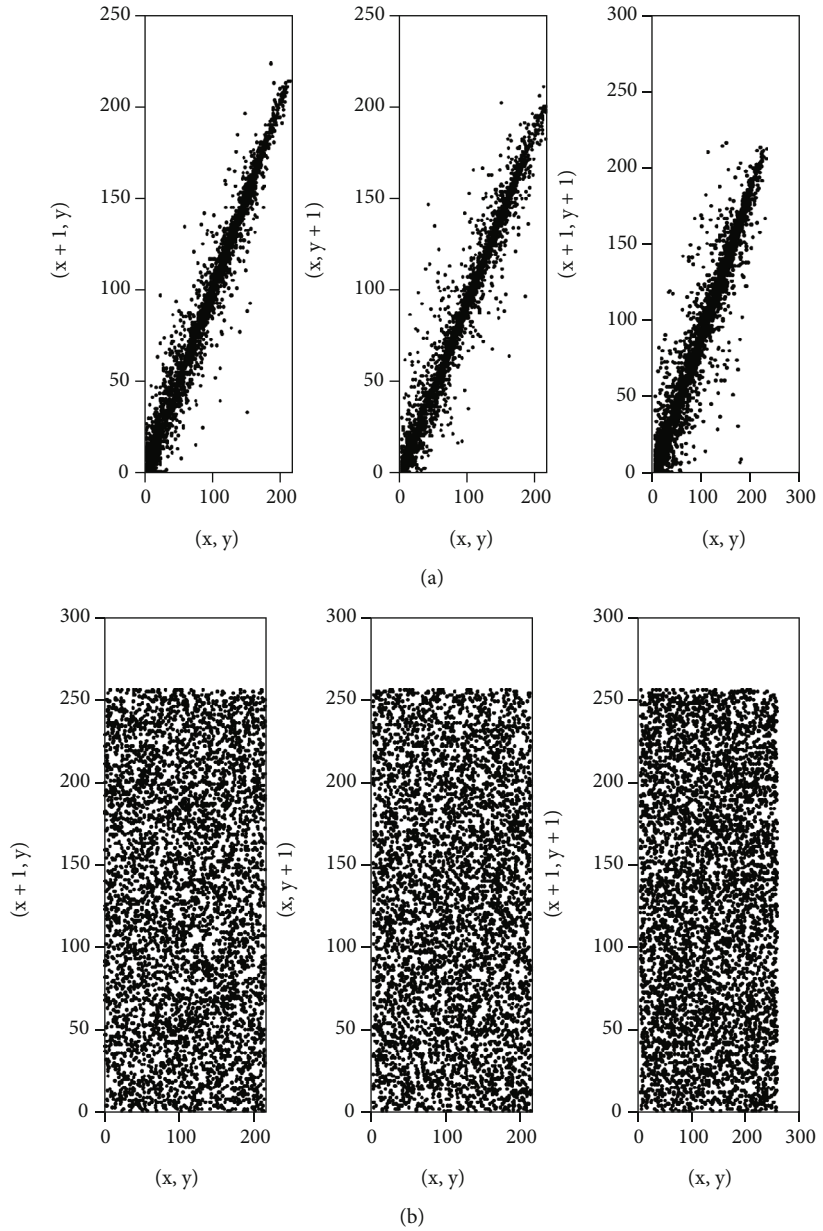


Figure 9: Correlation analysis of girl. (a) Correlation analysis of plaintext. (b) Correlation analysis of ciphertext.

Step 3: the first decryption is described as follows.
The decryption process of forward encryption:

$$\begin{aligned} C_2[S_3(m_1 \times n_1)] &= C_3[S_3(m_1 \times n_1)] - D_3[S_3(m_1 \times n_1)] \bmod 256, \\ C_2[S_3(i)] &= C_3[S_3(i)] - D_3[S_3(i)] - C_3[S_3(i+1)] \\ &\quad \cdot \bmod 256, \quad i = m_1 \times n_1 - 1, m_1 \times n_1 - 2, \cdots, 1. \end{aligned} \tag{12}$$

The decryption process of the backward encryption:

$$\begin{aligned} P[S_1(1)] &= C_2[S_1(1)] - D_1[S_1(1)] \bmod 256, \\ P[S_1(i)] &= C_2[S_1(i)] - D_1[S_1(i)] - C_2[S_1(i-1)] \\ &\quad \cdot \bmod 256, \quad i = 1, 2, 3, \cdots, m_1 \times n_1. \end{aligned} \tag{13}$$

Step 4: extract the face part $C_1 = P(a_1 : a_2, a_3 : a_4)$ for the second decryption

$$\begin{aligned} F[S_2(1)] &= C_1[S_2(1)] - D_2[S_2(1)] \bmod 256, \\ F[S2(i)] &= C_1[S2(i)] - D_2[S2(i)] - C_1[S2(i-1)] \\ &\quad \cdot \bmod 256, \quad i = 1, 2, 3, \cdots, m_2 \times n_2. \end{aligned} \tag{14}$$

Step 5: replace the first decrypted face part $P(a_1 : a_2, a_3 : a_4) = F$.
Output: P.

4. Simulation Experiments

4.1. Visualization. In the cryptographic system, select $\eta = 3.7$, $\theta = 5.2$, $\lambda = 2.6$, $x_0 = 0.65478466897887$, and $y_0 =$

Table 2: Correlation coefficients.

Image	Plaintext			Ciphertext		
	Hor.	Ver.	Diag.	Hor.	Ver.	Diag.
Barbara	0.861024	0.957077	0.840216	-0.000463	-0.001143	-0.000671
Girl	0.985419	0.988277	0.974804	0.000828	-0.000270	-0.005194
Lena	0.973730	0.986868	0.960985	-0.000904	0.000503	0.001368
Reagan	0.970919	0.979714	0.959251	0.0006615	0.003655	-0.000902

0.85426984531656 as the initial keys for visual analysis. The size of images are 512×512. The visual analysis result is shown in Figures 5–7. Visually, it has a good encryption effect, and the decryption algorithm can restore the plaintext image without loss.

4.2. NIST Statistical Tests. NIST is used to test whether plaintext images and ciphertext images are random. The NIST test results of the proposed algorithm are shown in Table 1. The NIST test results show that the pixel value of the plaintext image is not random, and the pixel value of the ciphertext has good randomness, so the algorithm has high security.

4.3. Correlation Analysis. The correlation coefficient of adjacent pixels can reflect the degree of diffusion of image pixel values. When adjacent pixel values have a low correlation and vice versa, the image presents a state of divergence. The lower the correlation, the better it can prevent the attacker from obtaining meaningful information from the ciphertext image. Figures 8 and 9 are the correlation analysis results of the proposed algorithm.

When the correlation image presents a state of aggregation, it indicates that the adjacent pixels of the image have strong correlation. When the correlation image shows a divergent state, it indicates that the adjacent pixels of the image have weak correlation. Visually, the proposed algorithm reduces the correlation of adjacent pixels in the image.

The quantitative analysis results of the correlation are shown in Table 2. In addition, the comparison results with some new methods (Nafise [27], Chai [7], Ayubi [28], and Asgar [29]) are shown in Table 3.

The relationship of plaintext image in three directions is linear, while the correlation of ciphertext is more discrete. The correlation analysis results show that the plaintext image has strong correlation, and the adjacent pixels of the ciphertext image basically have no correlation. The comparison results show that the proposed method has better effect and higher security.

4.4. Histogram Analysis. Generally speaking, the histogram is evenly distributed, which can effectively prevent attackers from analyzing the histogram to obtain plaintext information. Histogram analysis of the proposed method is shown in Figure 10. Histogram analysis shows that the distribution of ciphertext histograms is uniform, so the proposed algorithm can effectively mask the characteristics of plaintext images

Table 3: Correlation coefficient comparison of Lena.

Algorithms	Proposed	Nafise [27]	Chai [7]	Ayubi [28]	Asgar [29]
Hor.	-0.000904	-0.00055198	-0.0029	-0.0031	-0.0022
Ver.	0.000503	0.00086799	0.0013	-0.0293	0.0013
Diag.	0.001368	-0.0032701	-0.0026	0.0077	0.0013

The chi-square test was used to verify that the histogram was uniform [30], and the chi-square test results are shown in Table 4. The ciphertext chi-square test result is around 250, and the chi-square test result shows that the ciphertext histogram distribution is uniform.

4.5. Differential Attack. The cryptographic system should be sensitive to the plaintext. Even if the plaintext changes slightly, the obtained ciphertext should be very different. The two test indicators of NPCR and UACI are calculated as

$$\begin{aligned} \mathrm{NPCR} &= \frac{\sum_{i,j} E(i,j)}{M \times N} \times 100\%, \\ \mathrm{UACI} &= \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%. \end{aligned} \tag{15}$$

The size of images is 512×512, when the value of NPCR exceeds 99.5893% and the value of UACI is between 33.3730% and 33.5541%, indicating that the algorithm is resistant to differential attacks [31]. NPCR and UACI are shown in Table 5.

Differential attack results show that the algorithm proposed in this paper is sensitive to plaintext. Even if the plaintext changes slightly, the obtained ciphertext is also very different.

4.6. Key Analysis. The keys of the proposed algorithm include $x_0, y_0, \eta, \theta, \lambda$, and k_1. If the calculation accuracy is 10^{-15}, the key space of the proposed algorithm is

$$\begin{aligned} \mathrm{keyspace} &= 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \\ &\times 10^{15} = 10^{90} > 2^{100}. \end{aligned} \tag{16}$$

This is sufficient to resist brute force attacks. For different keys, even with minor changes, the final decrypted image should not contain any information related to the plaintext, that is, the algorithm is sensitive to the key. The sensitivity analysis of the algorithm is shown in

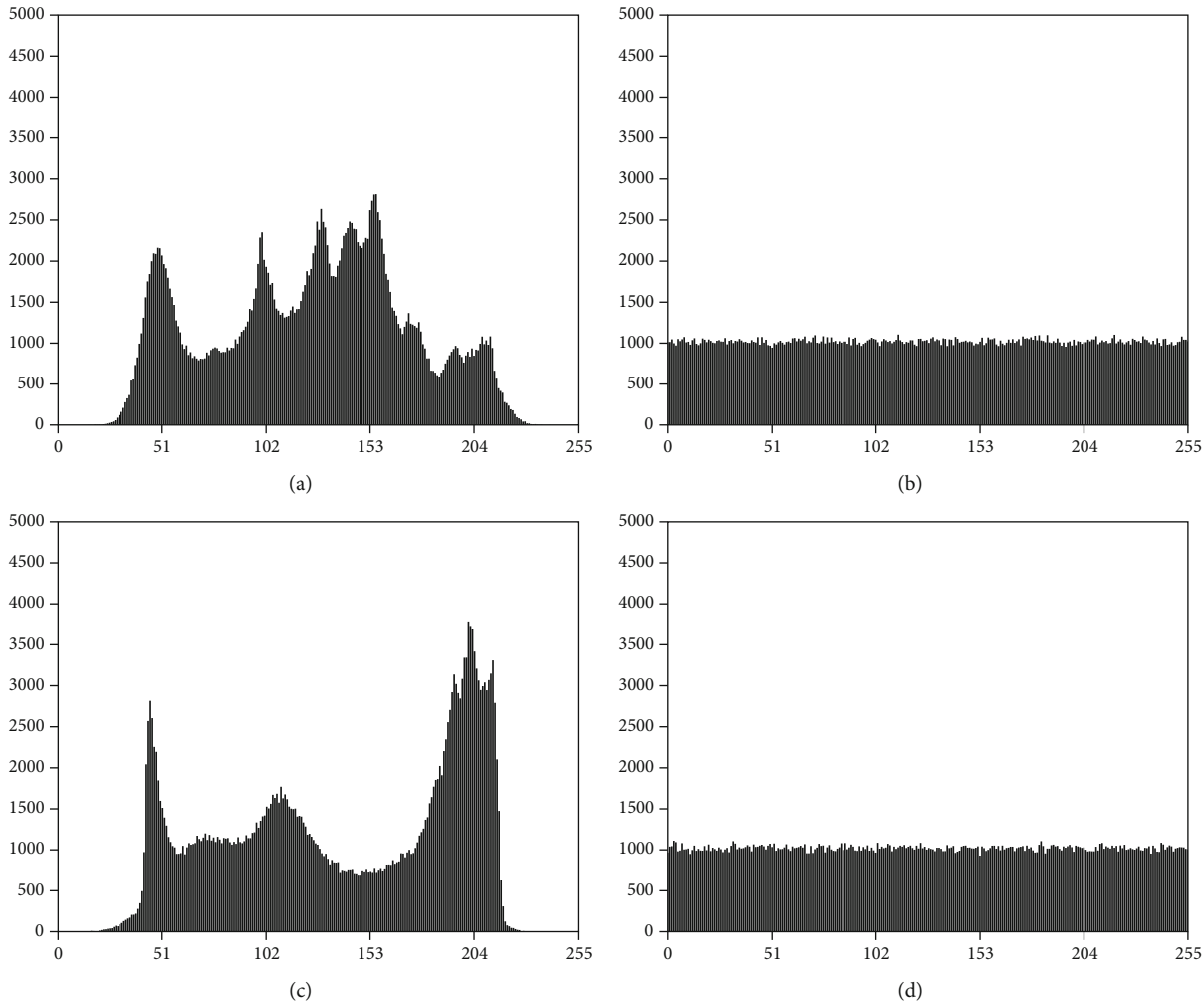


Figure 10: Histogram analysis. (a) Histogram analysis of Lena. (b) Histogram analysis of encrypted Lena. (c) Histogram analysis of Reagan. (d) Histogram analysis of encrypted Reagan.

Table 4: Chi-square test results.

Image	Plaintext	Ciphertext
Barbara	147977	267.1699
Girl	291918	264.4570
Lena	160082	244.4805
Reagan	212015	263.9355

Table 5: NPCR and UACI test results (%).

Image	NPCR	Pass or no pass	UACI	Pass or no pass
Barbara	99.6036	Pass	33.4892	Pass
Girl	99.6102	Pass	33.5023	Pass
Lena	99.6059	Pass	33.4652	Pass
Reagan	99.6099	Pass	33.4899	Pass

Figure 11. The initial keys are set to $\eta = 3.7$, $\theta = 5.2$, $\lambda = 2.6$, $x_0 = 0.65478466897887$, and $y_0 = 0.85426984531656$. The new keys are set to $\eta = 3.7 + 10^{-15}$, $\theta = 5.2 + 10^{-15}$, $\lambda = 2.6 + 10^{-15}$, $x_0 = 0.65478466897887 + 10^{-15}$, and $y_0 = 0.85426984531656 + 10^{-15}$.

Using NPCR and UACI to verify the difference in Figure 11, the sensitivity analysis results are shown in Table 6. Key sensitivity analysis shows that the image decrypted with the wrong key is very different from the plaintext image, indicating that the proposed algorithm has high sensitivity [32, 33].

4.7. Information Entropy Analysis. Information entropy is mainly used to measure the uncertainty of plaintext information and ciphertext information. For digital images, the calculation formula is

$$H(t) = -\sum_{i=0}^{255} p(t_i) \log p(t_i). \tag{17}$$

The information entropy of the proposed algorithm is shown in Table 7. In addition, the comparison results with some new methods (Nafise [27], Chai [7], Ayubi [28], and Asgar [29]) are shown in Table 8.

The local information entropy of the proposed algorithm is shown in Table 9. The local information entropy reflects

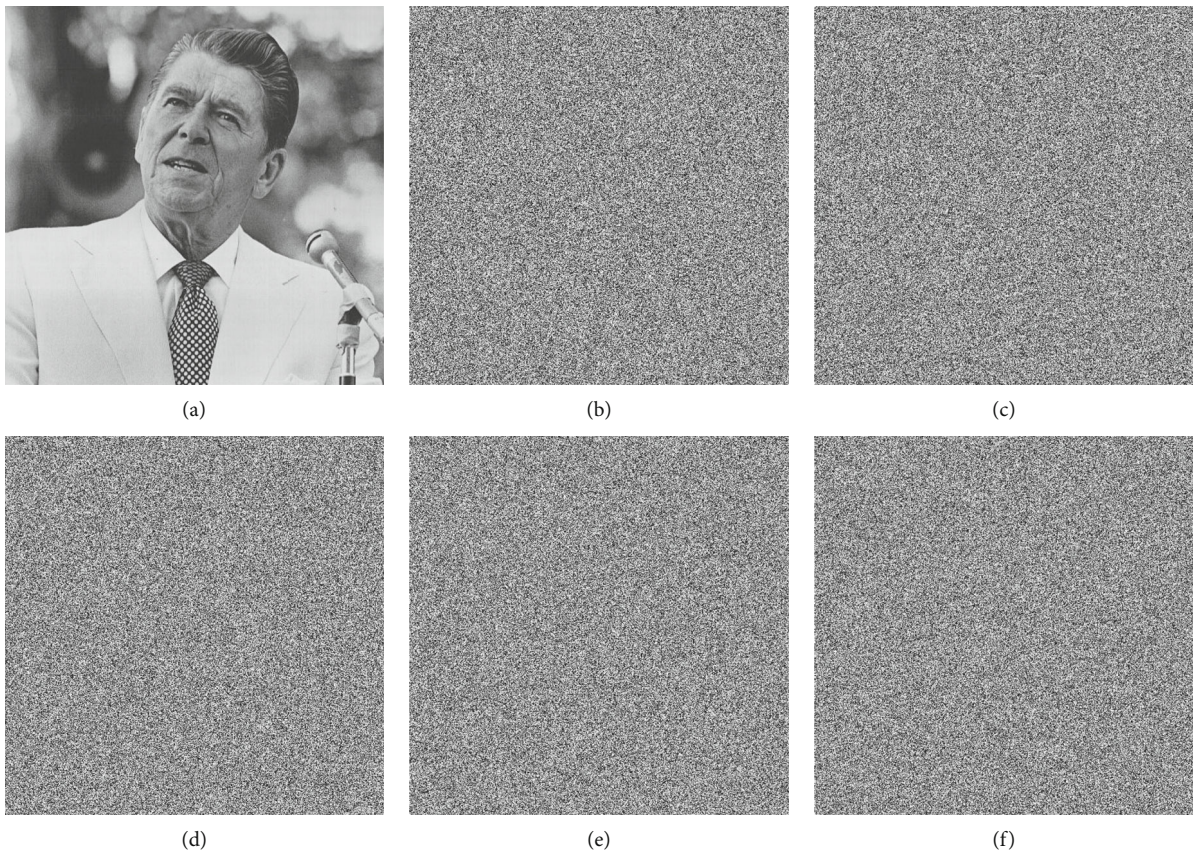


Figure 11: Sensitivity analysis. (a) Decrypted image by correct key. (b) Decrypted image by $x_0 = 0.65478466897887 + 10^{-15}$. (c) Decrypted image by $y_0 = 0.85426984531656 + 10^{-15}$. (d) Decrypted image by $\eta = 3.7 + 10^{-15}$. (e) Decrypted image by $\theta = 5.2 + 10^{-15}$. (f) Decrypted image by $\lambda = 2.6 + 10^{-15}$.

Table 6: Key sensitivity analysis (%).

NPCR/UACI	Figure 11(a)	Figure 11(b)	Figure 11(c)	Figure 11(d)	Figure 11(e)	Figure 11(f)
Figure 11(a)	—	0.304531	0.303453	0.304182	0.303810	0.304662
Figure 11(b)	0.995910	—	0.335992	0.335495	0.335304	0.336274
Figure 11(c)	0.996135	0.995716	—	0.336461	0.335448	0.336229
Figure 11(d)	0.995998	0.995811	0.995693	—	0.336208	0.337019
Figure 11(e)	0.996055	0.995536	0.995723	0.995811	—	0.336059
Figure 11(f)	0.996269	0.995491	0.995655	0.995841	0.995758	—

Table 7: Information entropy.

Image	Plaintext	Ciphertext
Barbara	7.460352	7.999264
Girl	7.251406	7.999273
Lena	7.448635	7.999328
Reagan	7.354212	7.999274

Table 8: Information entropy comparison of Lena.

Algorithms	Proposed	Nafise [27]	Chai [7]	Ayubi [28]	Asgar [29]
Information entropy	7.9993	7.9987	7.9973	7.9993	7.9984

Table 9: Local information entropy.

Image	Local information entropy	Result
Barbara	7.902155656540	Pass
Girl	7.902632365459	Pass
Lena	7.902423121654	Pass
Reagan	7.902232165444	Pass

the chaotic degree of the local information of the image. The range of the local information entropy is between 7.901901305 and 7.903037329 [34].

Information entropy analysis shows that the ciphertext of the proposed algorithm not only has better performance globally but also has better performance in local subblocks.

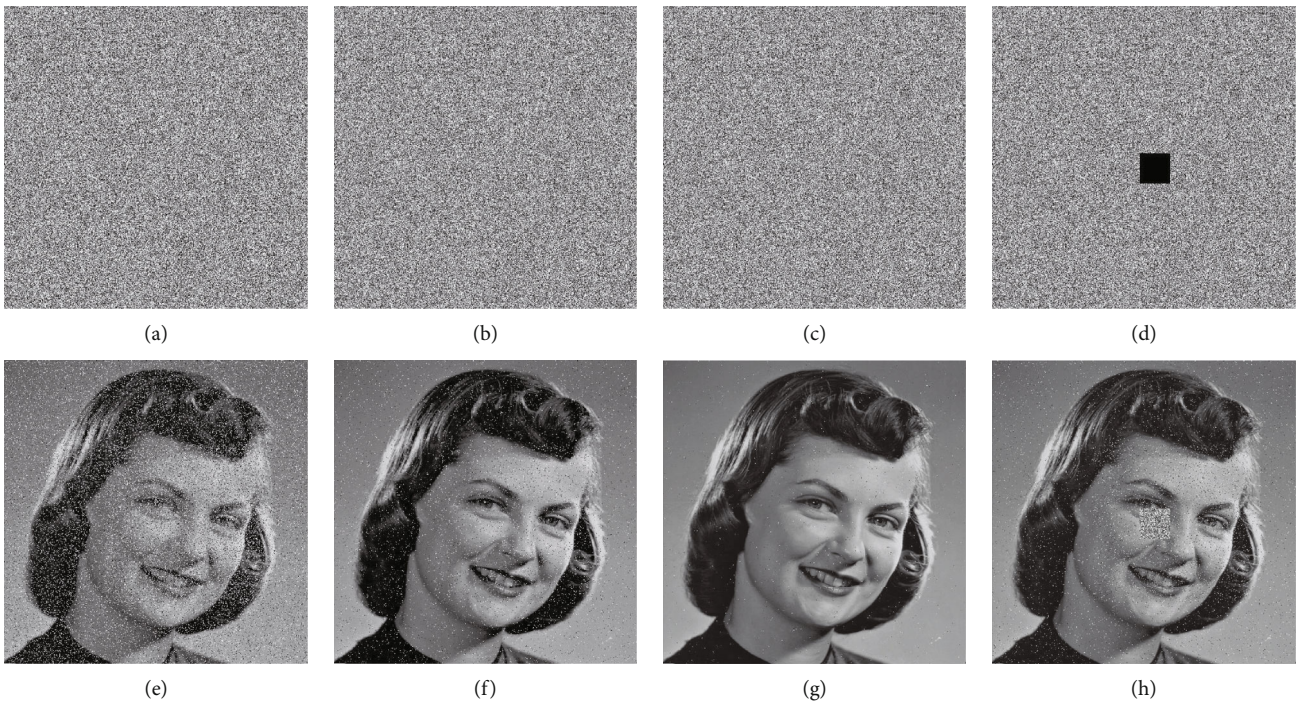


Figure 12: Robustness analysis. (a) 0.05 "salt & pepper." (b) 0.01 "salt & pepper." (c) 0.001 "salt & pepper." (d) Lose information. (e) Decrypt of 0.05 "salt & pepper." (f) Decrypt of 0.01 "salt & pepper." (g) Decrypt of 0.001 "salt & pepper." (h) Decrypt of lose information.

The comparative analysis results show that the information entropy of the proposed algorithm is closer to the theoretical value, so the proposed algorithm has higher security and resists statistical attacks.

4.8. Robustness Analysis. The plaintext will be attacked by some noise or lose some information during the transmission process, so the designed algorithm is required to be robust. Even under some noise attack or information loss, part of the plaintext image can still be obtained through the decryption algorithm. The robustness analysis of the algorithm is shown in Figure 12.

The Peak Signal-to-Noise Ratio (PSNR) metric is commonly used to measure the resiliency of an image and calculated as [35]

$$\mathrm{PSNR} = 10 \times \log \frac{255^2}{\mathrm{MSE}} (\mathrm{dB}). \tag{18}$$

Robustness of algorithms is tested by PSNR which are shown in Table 10.

The PSNR analysis results show that the proposed algorithm has good robustness. Even if part of the information is lost or attacked by noise, part of the plaintext information can still be obtained through the decryption algorithm. In addition, when the information is lost, although part of the information of the plaintext image is restored, the important information of the face is still in the ciphertext state, and this algorithm has a good effect on protecting the security of the face.

Table 10: PSNR of robustness analysis.

Image 1	Image 2	PSNR
Girl	Decrypt of 0.05 "salt & pepper"	14.6529
Girl	Decrypt of 0.01 "salt & pepper"	21.3457
Girl	Decrypt of 0.001 "salt & pepper"	31.0475
Girl	Decrypt of lose information	21.0327

Table 11: Speed analysis.

Algorithm	Time (s)
Proposed	0.336
Ref. [38]	0.663
Ref. [39]	0.390
Ref. [40]	0.785
Ref. [37]	0.139

4.9. Speed Analysis. The running time of the algorithm is also an important indicator for security analysis [36, 37]. The operating environment of the proposed algorithm is Windows 10, MATLAB 2021a, i3-10105, 4 cores, and 6 MB cache. The encryption time of the proposed algorithm is shown in Table 11.

The speed analysis shows that the encryption efficiency of the proposed algorithm is very fast, and it takes 0.336 s to process a 512×512 image. The experimental results show that the proposed algorithm is not only safe but also suitable for industrial production.

5. Conclusion

This paper proposes a double encryption strategy for images based on chaos. The face image is first identified, and the first encryption is to encrypt the identified face image. Combine the ciphertext with the original ciphertext to get a new plaintext image. The second encryption is to encrypt the entire image. In the design of the cryptographic system, we use the strategy of simultaneous diffusion and scrambling, which has high complexity. The double encryption algorithm has high security, and the attacker needs to crack two different encryption algorithms to obtain the original face image. Compared with cracking the algorithm once, there is no doubt that it is more difficult to crack twice. It is verified that the proposed algorithm has high security by NIST, visual analysis, statistical analysis, and other methods.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (61802212).

References

[1] H. Zhu, J. Ge, W. Qi, X. Zhang, and X. Lu, "Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system," *Mathematics and Computers in Simulation*, vol. 198, pp. 188–210, 2022.

[2] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[3] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "A new one-dimensional compound chaotic system and its application in high-speed image encryption," *Applied Sciences*, vol. 11, no. 23, p. 11206, 2021.

[4] S. Xu, X. Wang, and X. Ye, "A new fractional-order chaos system of Hopfield neural network and its application in image encryption," *Chaos, Solitons and Fractals*, vol. 157, article 111889, 2022.

[5] S. Zhou, X. Wang, M. Wang, and Y. Zhang, "Simple colour image cryptosystem with very high level of security," *Chaos, Solitons and Fractals*, vol. 141, article 110225, 2020.

[6] H. Liang, G. Zhang, W. Hou, P. Huang, B. Liu, and S. Li, "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography," *Applied Sciences*, vol. 11, no. 12, p. 5691, 2021.

[7] 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.

[8] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics and Laser Technology*, vol. 101, pp. 30–41, 2018.

[9] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, 2021.

[10] L. Geng, Y. Yu, and S. Zhang, "Dynamic analysis of the nonlinear chaotic system with multistochastic disturbances," *Journal of Applied Mathematics*, vol. 2014, 16 pages, 2014.

[11] W. Du, Y. Chu, J. Zhang, Y. Chang, J. Yu, and X. An, "Bifurcation analysis and sliding mode control of chaotic vibrations in an autonomous system," *Journal of Applied Mathematics*, vol. 2014, 14 pages, 2014.

[12] Y. Li, T. Zhang, and Y. Zhang, "Adaptive control of the chaotic system via singular system approach," *Journal of Applied Mathematics*, vol. 2014, 6 pages, 2014.

[13] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *PLoS One*, vol. 10, no. 3, article e0119660, 2015.

[14] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[15] 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, pp. 781–781, 2019.

[16] S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, "A novel image encryption cryptosystem based on true random numbers and chaotic systems," *Multimedia Systems*, vol. 28, no. 1, pp. 95–112, 2022.

[17] M. Abutaha, I. Amar, and S. AlQahtani, "Parallel and practical approach of efficient image chaotic encryption based on message passing interface (MPI)," *Entropy*, vol. 24, no. 4, p. 566, 2022.

[18] X. Han, X. Bi, B. Sun, L. Ren, and L. Xiong, "Dynamical analysis of two-dimensional memristor cosine map," *Frontiers in Physics*, vol. 10, 2022.

[19] Z. Yang, S. Yuan, J. Li, X. Bai, Z. Yu, and X. Zhou, "An encryption method based on computational ghost imaging with chaotic mapping and DNA encoding," *Journal of Optics*, vol. 24, no. 6, article 065702, 2022.

[20] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Optics and Lasers in Engineering*, vol. 125, p. 105851, 2020.

[21] 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.

[22] X. Wang, Y. Su, C. Luo, F. Nian, and L. Teng, "Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate," *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 13845–13865, 2022.

[23] G. Cheng, C. Wang, and C. Xu, "A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing," *Multimedia Tools and Applications*, vol. 79, no. 39-40, pp. 29243–29263, 2020.

[24] N. Zhou, W. Chen, X. Yan, and Y. Wang, "Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system," *Quantum Information Processing*, vol. 17, no. 6, pp. 1–24, 2018.

[25] D. Wei and M. Jiang, "A fast image encryption algorithm based on parallel compressive sensing and DNA sequence," *Optik*, vol. 238, p. 166748, 2021.

[26] W. Liu, K. Sun, and S. He, "SF-SIMM high-dimensional hyperchaotic map and its performance analysis," *Nonlinear Dynamics*, vol. 89, no. 4, pp. 2521–2532, 2017.

[27] N. R. Pour and M. Yaghoobi, "A new method in encryption of gray scale images using chaos game representation," *Multimedia Tools and Applications*, 2022.

[28] P. Ayubi, S. Setayeshi, and A. M. Rahmani, "Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, vol. 52, p. 102472, 2020.

[29] M. Asgari-Chenaghlu, M. A. Balafar, and M. R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1–13, 2019.

[30] D. Ravichandran, P. Praveenkumar, J. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[31] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology," *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[32] 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.

[33] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Computers and Electrical Engineering*, vol. 54, pp. 471–483, 2016.

[34] 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.

[35] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Optics and Laser Technology*, vol. 114, pp. 224–239, 2019.

[36] E. Yavuz, "A new parallel processing architecture for accelerating image encryption based on chaos," *Journal of Information Security and Applications*, vol. 63, p. 103056, 2021.

[37] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 60, pp. 12–32, 2018.

[38] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[39] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 639–653, 2016.

[40] F. K. Mohamed, "A parallel block-based encryption schema for digital images using reversible cellular automata," *Engineering Science and Technology, an International Journal*, vol. 17, no. 2, pp. 85–94, 2014.