Multimedia Tools and Applications (2021) 80:11655–11670
https://doi.org/10.1007/s11042-020-10202-2

Bit-level image encryption algorithm based on BP neural network and gray code

Xingyuan Wang[1] · Shujuan Lin[1] · Yong Li[1]

Received: 6 September 2019 / Revised: 30 September 2020 / Accepted: 24 November 2020 /
Published online: 6 January 2021

Abstract
In recent years, people have put forward various image encryption algorithms based on pixel level. In fact, bit level encryption has better effect than pixel level encryption. Therefore, this paper proposes a new bit-level image encryption algorithm based on Back Propagation (BP) neural network and Gray code. Firstly, the plaintext image is conversioned into binary image, then, the hyperchaotic Lorentz system is used to generate two sets of chaotic sequences for the Gray code bit-level permutation operation to generate the permutation matrix. Secondly, the permutation matrix is converted into a bit matrix reverse order output to generate a diffusion matrix. Finally, the algorithm uses a BP neural network composed of Logistic map and Piece-Wise Linear Chaotic (PWLCM) map to generate a key stream. The key stream is xored with the diffusion matrix to generate a ciphertext matrix. The experimental results show that the algorithm improves the encryption efficiency, has good security and can resist common attack methods.

Keywords BP neural network · Gray code · Hyperchaotic Lorentz system · Bit-level · Image encryption

1 Introduction

With the rapid development of the Internet and multimedia technologies, people are paying more and more attention to information security issues. Among them, images, as carriers of information security, have high requirements for security and confidentiality. Although traditional encryption algorithms (such as DES and RSA) can be used for image encryption, they have large capacity, high redundancy, and high pixel correlation, which are not suitable for

✉ Xingyuan Wang
xywang@dlmu.edu.cn

Shujuan Lin
2450274321@qq.com

[1] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China

image encryption. Therefore, a good image encryption algorithm is essential. Good image encryption schemes have been proposed, for example, DNA sequences [6, 13, 29], coupled map lattices [8, 15, 32], S-boxes [3, 7, 36], wavelet transforms [4], chaotic systems and the like [2, 5, 22, 28]. Among them, chaos plays an important role. Chaos is a theoretical system that is very sensitive to the initial state, and has a high degree of randomness and mixing. It is the most widely used system for image encryption.

In recent years, more and more chaotic systems have been used for image encryption, and some chaotic-based image encryption algorithms have also been well developed. For example, based on DNA sequences [23, 34, 35], based on a hybrid chaotic map or a high-dimensional chaotic system [24, 25, 31], based on Fisher-Yates [26], and image encryption algorithm based on bit-level permutation [11, 14, 16]. Compared with pixel-level permutation, bit-level permutation not only changes the position of the pixel, but also changes the value of the pixel, which has better encryption effect. At present, more and more bit-level-based encryption schemes have been proposed. For example, Zhou et al. proposed Bit-level quantum color image encryption scheme [37], Xu et al. proposed bit-level image encryption based on chaotic mapping [30], Zhang et al. proposed a bit-level image encryption algorithm based on rotation matrix and block diffusion [33].

In recent years, neural network has been widely integrated into image encryption, and its distributed parallel information processing has improved the efficiency of image encryption. For example, Wang et al. proposed a color image encryption algorithm based on hopfield chaotic neural network [20], Ratnavelu et al. proposed image encryption method based on chaotic fuzzy cellular neural networks [12], Wei et al. proposed stability of stochastic impulsive reaction-diffusion neural networks with S-type distributed delays and its application to image encryption [27], Ahmad et al. proposed cryptanalysis of an image encryption algorithm based on PWLCM and inertial delay neural network [1]. and Wang et al. proposed schemes of applying boolean networks to image encryption [17, 18]. Gray code is a kind of reliability coding of binary conversion. It will be a good combination to apply it synchronously with neural network in image encryption.

This paper proposes a bit-level image encryption algorithm based on BP neural network and Gray code. In the permutation, the Gray code is used for the bit-level permutation operation. In the diffusion, the bit-level reverse-order output is first adopted, and then the chaotic map is outputted through the BP neural network model for the divergence xor operation. After a lot of experimental tests, the algorithm can be used for image encryption and it works well.

The rest of the paper is arranged as follows. The second chapter introduces the chaotic system and replacement methods used in this paper. The third chapter introduces the process description of the encryption algorithm. The fourth chapter shows the simulation results of image encryption. The fifth chapter has carried out a large number of experimental tests on the algorithm. The sixth chapter is the conclusion of this paper.

2 Related method

2.1 System and chaotic map

2.1.1 Hyperchaotic Lorenz system

The Lorenz system is a hyperchaotic system with a positive Lyapunov exponent [21]. The dynamic behavior of the system is difficult to predict. The dynamic equation is:

$$\begin{cases} x = a(y - x) + w \\ y = cx - y - xz \\ z = xy - bz \\ w = -yz + rw \end{cases}. \tag{1}$$

When $a = 10$, $b = 8/3$, $c = 28$, and $-1.52 < r \leq -0.06$, the hyperchaotic Lorenz system has a positive Lyapunov exponent in a hyperchaotic state. The resulting sequence is aperiodic, non-convergent and very sensitive to initial values.

2.1.2 Logistic map

The Logistic map is a one-dimensional chaotic system [10], whose equation is:

$$x_{n+1} = ux_n(1 - x_n). \tag{2}$$

Among them $x_n \in (0, 1)$, when the parameters are $\mu \in (3.5699456, 4]$, the Logistic map is chaotic, and the generated sequence $\{x_n, n = 0, 1, 2, 3\ldots\}$ is aperiodic, non-converged, and very sensitive to the initial value. In order to avoid the periodic window, this paper uses the parameters in the range of $u \in (3.89,4]$.

2.1.3 PWLCM map

The PWLCM map is a map composed of multiple linear segments [19], which has a more balanced nature than the Logistic map. The dynamic equation is:

$$x_{n+1} = F(x_n) = \begin{cases} x_n/p, 0 \leq x_n < p \\ (x_n - p)/0.5 - p, p \leq x_n < 0.5 \\ F[1 - x_n], 0.5 \leq x_n < 1 \end{cases}. \tag{3}$$

The control parameters $P \in (0,0.5)$, x_n and x_{n+1}, are the input and output states of the chaotic map during system iteration, both of which are within the interval of (0.1). In this paper, the control parameters are limited to (0.2,0.3) and have better chaotic characteristics than the entire control range.

2.2 BP neural network

The Back Propagation [9], proposed by the team of scientists led by Rumelhart and McCelland in 1986, is a multi-layer feedforward network trained by error inverse propagation algorithm and is one of the most widely.

used neural network models. The BP neural network consists of three parts: input layer, hidden layer and output layer. In this paper, the pixels of the plaintext image are processed and used as the input of the neural network,

while the hidden layer is placed into Eqs. (2) and (3) as the transfer function. Finally, the output layer outputs a.

set of random sequences as the key stream of the encryption process. Its BP neural network model is shown in Fig. 1.

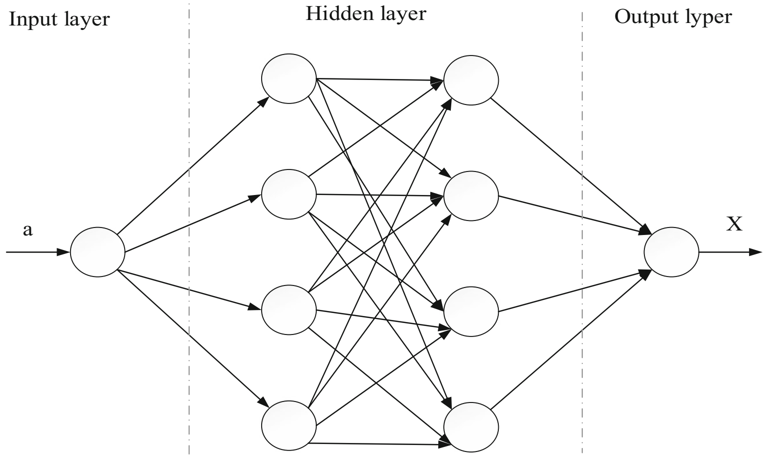


Fig. 1 BP neural network

2.3 Bit level image

In grayscale images, the brightness between black and white is quantized to an integer number of levels between 0 and 255. Each pixel value can be converted to an 8-bit binary. The plaintext image can be divided into 8 bit-level images according to the binary position. The position of the bit value is different, and the amount of information stored is different. The high 4-bit image stores 94.125% of the plaintext information, and the other 6% of the information is stored in the lower 4-bit image. We selected the "Lena" image to test the 8-bit-level image. The 8 bit-level images of Lena image be shown in Fig. 2.

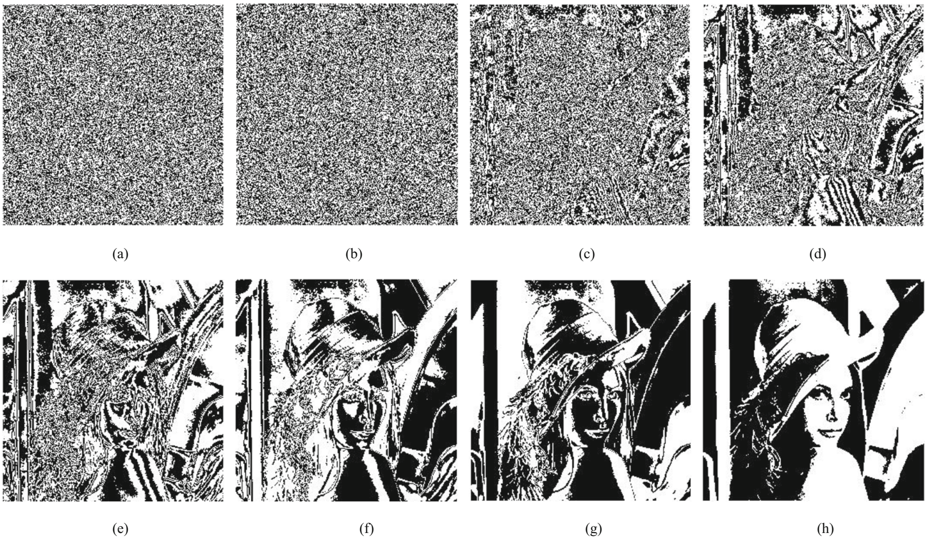


Fig. 2 The 8 bit-level images of Lena image (**a**) Bit plane 1 (**b**) Bit plane 2 (**c**) Bit plane 3 (**d**) Bit plane 4 (**e**) Bit plane 5 (**f**) Bit plane 6 (**g**) Bit plane 7 (**h**) Bit plane 8

2.4 Gray code

Gray code, also known as cyclic binary code or reflection binary code, it is a coding method that we often encounter in engineering. Its basic feature is that any two adjacent codes have only one binary number. This paper takes the conversion between binary and Gray code. The binary code is converted into Gray code, the rule is to reserve the highest bit of the binary code as the highest bit of the Gray code, and the second highest bit Gray code is obtained by xoring the high and the second highest bits of the binary code. The Gray code is converted into a binary code, the rule is to reserve the highest bit of the Gray code as the highest bit of the natural binary code, and the second highest natural binary code is obtained by xoring the high natural binary code with the next highest order Gray code. Table 1 shows the conversion relationship between Gray code and binary code.

3 Encryption process description

3.1 High 4-bit image permutation

Due to the high 4-bit image stores most of the plaintext information, the high 4-bit image is first replaced.

Step 1: The plaintext image P of $M \times N$ is converted into a binary image according to Eq. (4), and the high 4-bit and the lower 4-bit are separated according to Eq. (5), the high 4-bit image is A_1, and the lower 4-bit image is A_2.

$$P = de2bi(P). \tag{4}$$

$$A_1 = P(:, 1:4), A_2 = P(:, 5:8). \tag{5}$$

Step 2: The *sum* of all the values of the high 4-bit matrix is obtained according to the Eq. (6), and the sum is processed according to the Eq. (7) to generate the variable a as the input value of the BP neural network.

$$sum = sum(A_1(:)). \tag{6}$$

Table 1 The conversion relationship between Gray code and binary code

Decimal code	0	1	2	3	4	5	6	7
Binary code	0000	0001	0010	0011	0100	0101	0110	0111
Gary code	0000	0001	0011	0010	0110	0111	0101	0100
Decimal code	8	9	10	11	12	13	14	15
Binary code	1000	1001	1010	1011	1100	1101	1110	1111
Gary code	1100	1101	1111	1110	1010	1011	1001	1000

$$a = mod((1/sum), 1). \tag{7}$$

Step 3: Performing a Gray code permutation operation on the rows and columns of the high 4-bit image according to Eqs. (8) and (9) to generate a high 4-bit change matrix B_1.

$$B_1(:, \mathrm{j}) = xor(A_1(:, \mathrm{j}), A_1(:, \mathrm{j}{-}1)). \tag{8}$$

$$B_1(i, :) = xor(B_1(i, :), B_1(i{-}1, :)). \tag{9}$$

Step 4: The high 4-bit change matrix B_1 and the low 4-bit matrix A_2 are combined into the matrix B according to the Eq. (10).

$$B = [B_1, A_2]. \tag{10}$$

3.2 Global permutation

Due to the Gray code permutation has the defect that the first value does not change, and the lower 4-bit image still stores 6% of the plaintext information, this paper chooses to perform a global permutation on the matrix B.

Step 1: First, the Lorentz system is iterated $M \times N + 500$ times into a set of chaotic sequence AA according to Eq. (1), and the first 500 chaotic values are discarded to avoid transient effects. Due to the chaotic sequence generated by the Lorentz system have minus, then the chaotic sequence is normalized to the range of (0, 1), and the index matrix I is generated according to the Eq. (11).

$$[S, I] = sort(AA). \tag{11}$$

Step 2: The matrix B is globally permuted according to Eq. (12), and a permutation matrix B_2 is generated.

$$B_2(j, i) = B(I(i, j), i). \tag{12}$$

Step 3: The permutation matrix B_2 is converted into a decimal matrix according to a Eq. (13).

$$B_2 = bi2de(B_2). \tag{13}$$

3.3 Bit-level diffusion

Step 1: The decimal matrix B_2 is converted into a bit-level matrix G according to Eq. (14).

$$G = dec2bin(B_2). \tag{14}$$

Step 2: Each bit of the bit-level matrix G is output in reverse order according to Eq. (15) to generate a diffusion matrix G_1, and then the bit-level matrix is converted into a decimal matrix according to Eq. (16).

$$G_1 = G(:, 8 : -1 : 1). \tag{15}$$

$$G_1 = bin2dec(G_1). \tag{16}$$

Step 3: The input value a is iterated $M \times N + 500$ times by Eq. (2) to generate a set of sequence, and the first 500 chaotic values are discarded to avoid transient effects. The generated sequence is passed by the second hidden layer according to Eq. (3) to generate a set of $M \times N$ sequences X.

Step 4: The X is processed according to Eq. (17) to generate a key stream K required for diffusion.

$$K = floor\left(\mathrm{mod}\left(X \times 10^{16}\right), 256\right). \tag{17}$$

Step 5: Due to the bit reverse order diffusion operation cannot change the pixel with the value of 255, a round of diffusion operation is performed in this paper, and the diffusion matrix G_1 and the key stream K are xored according to the Eq. (18) to generate the ciphertext matrix C.

$$C = bitxor(G_1, K). \tag{18}$$

Since the decryption process is the inverse of encryption, it will not be described here.

4 Simulation results and performance analysis

4.1 Simulation results

This paper uses Matlab 2017 to encrypt five plaintext images of “Lena”, “Peppers”, “Cameraman”, “Girl” and “Finger”. Figure 3 shows the effect of encryption and decryption of three images. It can be seen from Fig. 3 that the encrypted image can not see any information of the original image at all, so visually, the algorithm has achieved a better encryption effect.

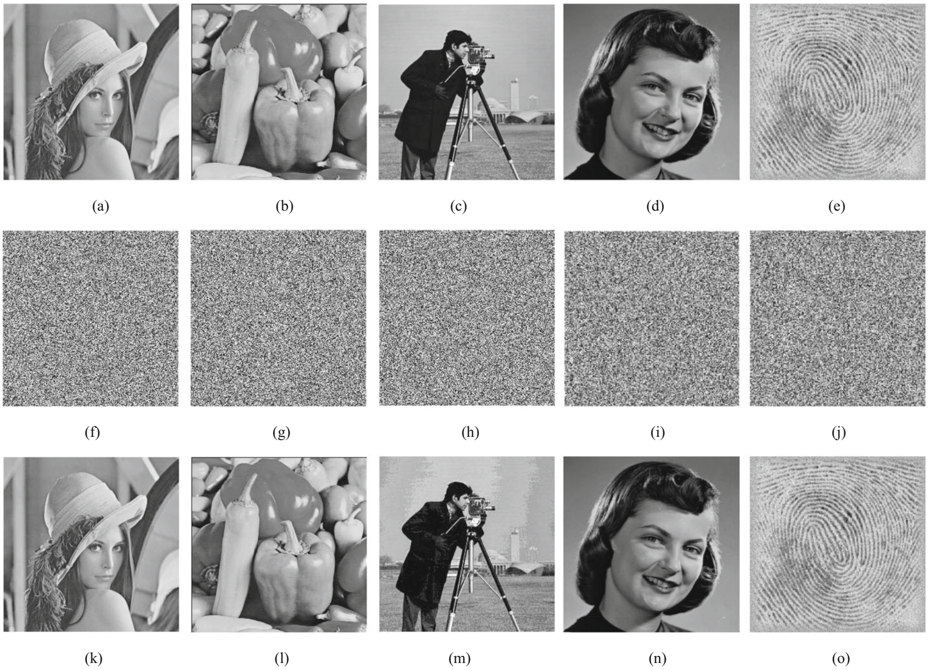


Fig. 3 Encryption and decryption of gray-scale image (**a**) Plaintext Lena (**b**) Plaintext Pepper (**c**) Plaintext Cameraman (**d**) Plaintext Girl (**e**) Plaintext Finger (**f**) Ciphertext of Lena (**g**) Ciphertext of Pepper (**h**) Ciphertext of Cameraman (**i**) Ciphertext of Girl (**j**) Ciphertext of Finger (**k**) Decryption of Lena (**l**) Decryption of Pepper (**m**) Decryption of Cameraman (**n**) Decryption of Girl (**o**) Decryption of Finger

4.2 Key space analysis

In this paper, the non-integer key precision can reach 10^{-14}, and the key space can be greater than 2^{100}, which can achieve theoretical non-violent cracking. In addition, this paper also conducted related experiments on the sensitivity of the key. The experiment uses the original

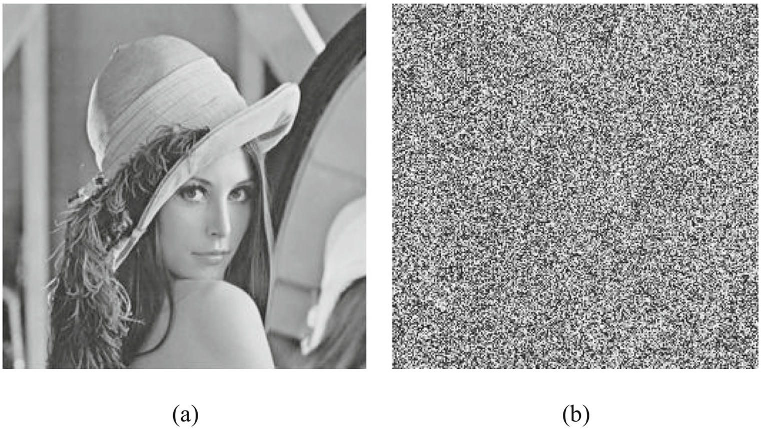


Fig. 4 Sensitivity of secret key (**a**) Correct key restoring diagram (**b**) Error key restoring diagram

key to encrypt the plaintext to obtain the ciphertext image, and decrypts it using the correct key and the slightly changed error key. Figure 4 shows the test results. In Fig. 4a, the correct key is used for decryption, and the resulting image is identical to the original plaintext image. In Fig. 4b, the key is decrypted using a slightly changed key, and the resulting image is completely different from the original plaintext. As can be seen from the decryption results, even if the key has a very small change, the result obtained by the algorithm decryption is completely different. Therefore, the algorithm has high sensitivity to the initial key and has good security against statistical analysis attacks.

4.3 Statistical analysis

Statistical analysis is to use statistical methods to verify the encryption effect of images. The statistical methods used in this paper include histogram analysis and correlation analysis.

4.3.1 Histogram analysis

The histogram is a graph reflecting the frequency of the pixel value information in the image. When the histogram of the encrypted image shows a state in which all the pixel values are uniform, the encryption effect is good and the statistical analysis can be resisted. Figure 5 shows the plaintext and ciphertext histograms for the five images "Lena", "Peppers", "Cameraman", "Girl" and "Finger". It can be seen from Fig. 6 that all the encrypted histograms of five images selected in this paper are in a straight line state, that is, the pixel value information of the encrypted image is uniformly distributed, and the algorithm achieves a better encryption effect.

4.3.2 Correlation analysis

In the plaintext image, adjacent pixels have a high correlation. To avoid image information being attacked, the correlation between adjacent pixels should be reduced. When the correlation coefficient is close to zero, the algorithm can resist statistical analysis. Pixel correlation analysis includes three directions, vertical, horizontal and diagonal.

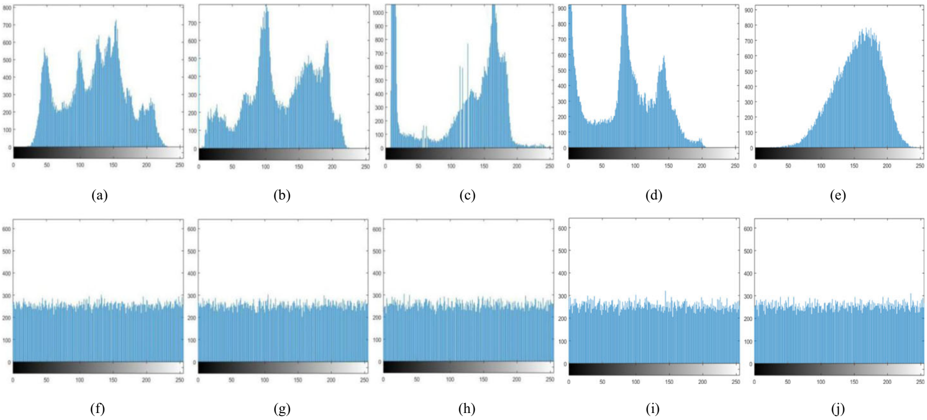
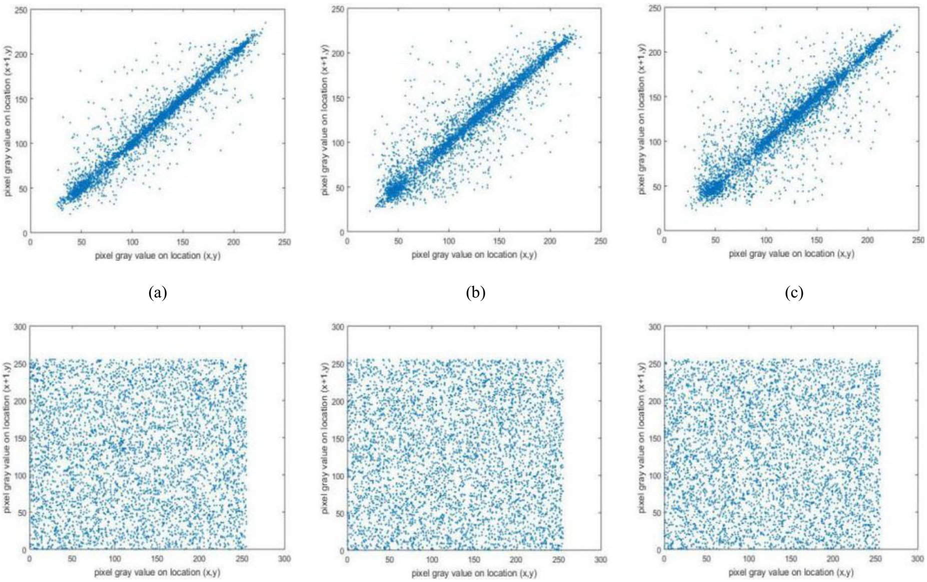


Fig. 5 Histograms of plain images and ciphered images (**a**) Histogram of Lena (**b**) Histogram of Peppers (**c**) Histogram of Cameraman (**d**) Histogram of Girl (**e**) Histogram of Finger (**f**) ciphered Lena (**g**) ciphered Peppers (**h**) ciphered Cameraman (**i**) ciphered Girl (**j**) ciphered Finger



(a)

(b)

(c)

(d)

(e)

(f)

Fig. 6 Correlation coefficients of Lena (**a**) Horizontal correlation of plain image (**b**) Vertical correlation of plain image (**c**) Diagonal correlation of plain image (**d**) Horizontal correlation of ciphered image (**e**) Horizontal correlation of ciphered image (**f**) Diagonal correlation of ciphered image

$$rxy = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{19}$$

among them.

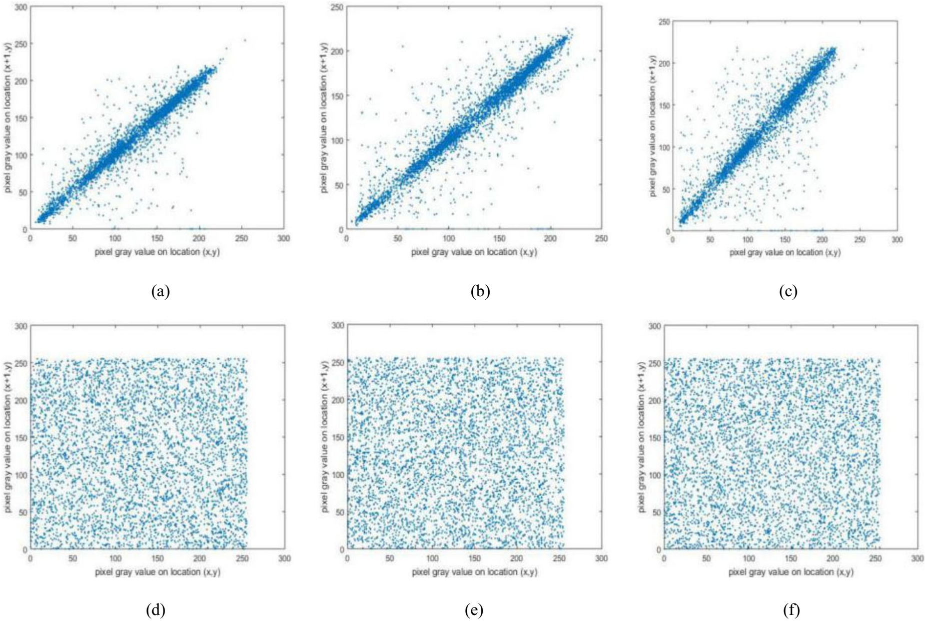
$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i.$$

x, y are the gray value of two adjacent pixels. This paper selects 2000 pairs of pixels according to the Eq. (19) to test the “Lena”, “Peppers”, “Cameraman” image of the plaintext image and the ciphertext image horizontal, vertical, diagonal direction correlation, as shown in Figs. 6, 7, 8. It can be seen from the ciphertext correlation in Figs. 6, 7, 8 that the pixel values of ciphertext images are uniformly distributed in both horizontal, vertical and diagonal directions.

Table 2 shows the correlation coefficients of the five plaintext images and the ciphertext images of “Lena”, “Peppers”, “Cameraman”, “Cirl” and “Finger”. Experiments show that the algorithm can resist statistical analysis when the correlation coefficient is close to zero. Compared with the Lena image in Ref. [3], Ref. [2], Ref. [1], we can see that there is no significant difference between the algorithm and the three documents. Therefore, It can be seen from the table that the algorithm is feasible.

4.4 Information entropy analysis

Information entropy reflects the degree of confusion of image pixels. When the information entropy is close to 8, it indicates that the pixel values in the image are disordered (Table 3).

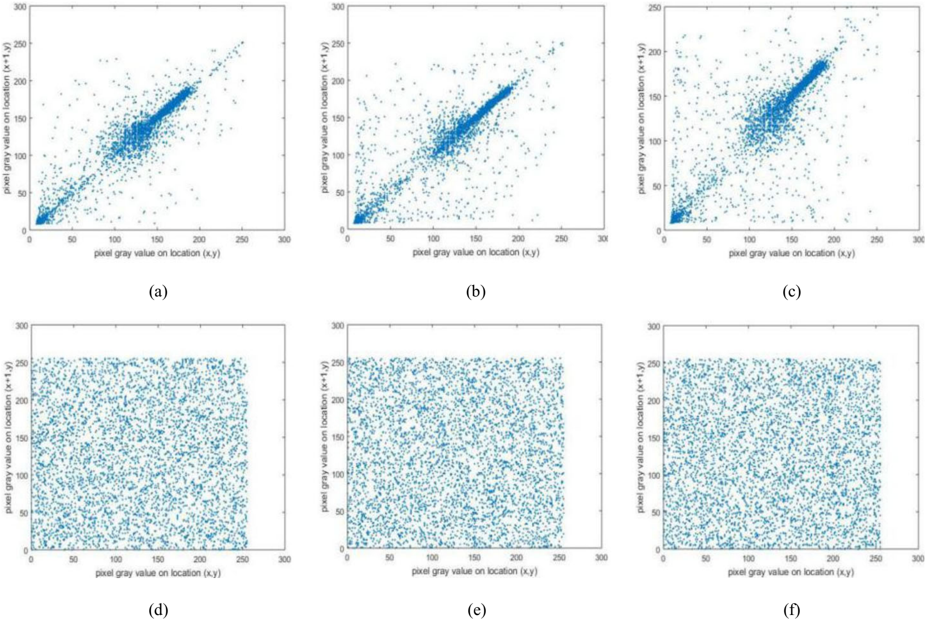


(a) (b) (c)

(d) (e) (f)

Fig. 7 Correlation coefficients of Peppers (**a**) Horizontal correlation of plain image (**b**) Vertical correlation of plain image (**c**) Diagonal correlation of plain image

$$H(s) = \sum_{i=0}^{2^L-1} p(s_i) log_2 \frac{1}{p(s_i)}. \tag{20}$$



(a) (b) (c)

(d) (e) (f)

Fig. 8 Correlation coefficients of Cameraman (**d**) Horizontal correlation of ciphered image (**e**) Horizontal correlation of ciphered image (**f**) Diagonal correlation of ciphered image

Table 2 Correlation coefficients of images

Image	Horizontal	Vertical	Diagonal
Plaintext Lena	0.9384	0.9682	0.9129
Plaintext Peppers	0.9593	0.9642	0.9324
Plaintext Cameraman	0.9335	0.9591	0.9083
Girl	0.9704	0.9761	0.9504
Finger	0.5583	0.6161	0.5097
Ciphertext Lena	5.9231e- 04	3.5043e- 04	0.0020
Ciphertex Peppers	0.0026	9.6231e- 04	0.0029
Ciphertex Cameraman	7.0828e- 04	0.0024	2.8855e- 04
Ciphertex Girl	7.6782e- 04	0.0016	−0.0034
Ciphertex Finger	−0.0023	−0.0011	−0.0010
Lena in Ref. [3]	- 0081	- 0.0037	0.0088
Lena in Ref. [2]	- 0.0017	- 0.0084	- 0.0019
Lena in Ref. [9]	0.00046	0.0011	- 0.0031

Where $p(s_i)$ represents the probability of s_i occurring. The information entropy of the "Lena", "Peppers", "Cameraman", "Cirl" and "Finger" plaintext images and ciphertext images was tested according to Eq. (20), It can.

be seen from the table data that the entropy value of image information encrypted by this algorithm has reached 7.99, which is equivalent to infinite close to 8, which indicates that the pixel value has reached a good degree of chaos. Compared with the Lean image in Ref. [3], Ref. [2] and Ref. [1], the data in the table further verify the validity of the algorithm.

4.5 Differential attack analysis

The differential attack is to make a slight change to a pixel value in the plaintext image, and then encrypt it with the encryption scheme of this paper. The differential attack includes NPCR and UACI. NPCR represents the rate of change in the number of pixels of the image, and UACI represents the average intensity of the difference between the normal image and the encrypted image. When the NPCR reaches 99.6% and the UACI reaches 33.4%, it can resist differential attacks (Table 4).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100. \tag{21}$$

Table 3 Information entropy of images

Image	Plain	Proposed
Lena	7.4445	7.9975
Peppers	7.5326	7.9975
Cameraman	6.9718	7.9973
Girl	7.2574	7.9968
Finger	7.1075	7.9971
Lena in Ref. [3]	7.4456	7.9993
Lena in Ref. [2]	7.5764	7.9975
Lena in Ref. [9]	–	7.9976

Table 4 The average of NPCR and UACI and comparison with other algorithms

Image	NPCR (%)	UACI (%)
Lena	99.6078	33.5309
Peppers	99.6200	33.4506
Cameraman	99.6215	33.3309
Girl	99.6170	33.4282
Finger	99.5986	33.4275
Lena in Ref. [3]	99.61	33.52
Lena in Ref. [2]	99.620	33.505
Lena in Ref. [9]	99.6155	28.567

$$UACI = \frac{1}{W \times H} = \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255}\right] \times 100. \tag{22}$$

Where W and H represent the width and height of the image, respectively, c_1 and c_2 are the two ciphertext images after the original plaintext image changes by one pixel value. If $c_1(i,j) \neq c_2(i,j)$, then $D(i,j) = 1$, otherwise $D(i,j) = 0$. According to Eqs. (21) and (22), we tested NPCR and UACI of five grayscale images of "Lena", "Peppers", "Cameraman", "Cirl" and "Finger", The data in the table show that the NPCR and UACI of the encrypted image reach the standard

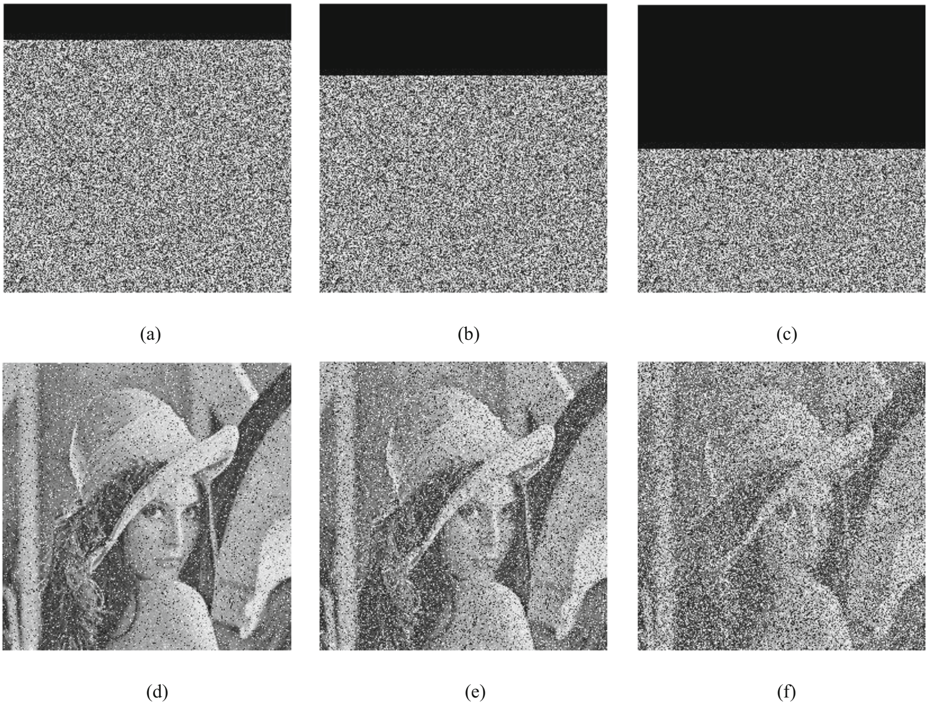


Fig. 9 Cropping attack analysis (**a**) Full encryption 1/8 block attack (**b**) Full encryption 1/4 block attack (**c**) Full encryption 1/2 block attack (**d**) Decryption image of (**a**) (**e**) Decryption image of (**b**) (**f**) Decryption image of (**c**)

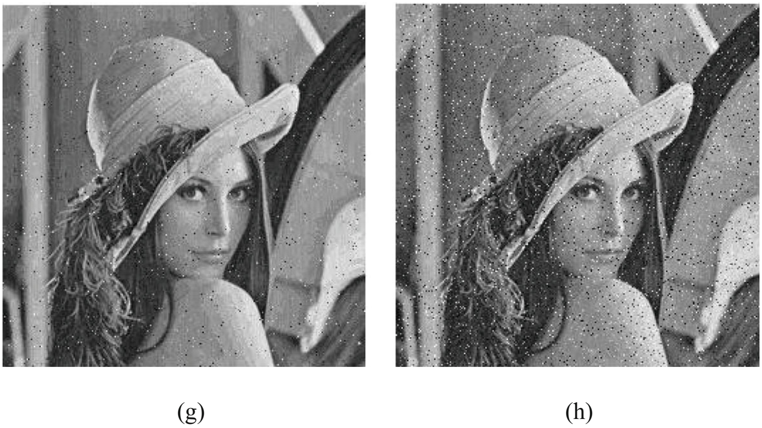


Fig. 10 Noise attack analysis (**g**) Decryption image of 0.01 salt & pepper (**h**) Decryption image of 0.05 salt & pepper

value. And compared with the lena image in Ref. [3], Ref. [2] and Ref. [1], both data can effectively verify that the algorithm is feasible.

4.6 Cropping attack and noise attack analysis

Images are easily hijacked during communication, and once the information in the image has been tampered with, it will be irreparable. To prevent this, the ciphertext should have good resistance to cropping attacks. Test ciphertext's anti-cutting attack capabilities, cropping attacks and noise attacks are the two most common methods. In this paper, the ciphertext image is cut by 1/2, 1/4, 1/8 information to test the robustness of the encryption system. This paper tested the cropping and noise attacks of the "Lena" image. Figures 9 and 10 show the clipping and noise attacks of the "Lena" image respectively. Whether clipping or noise attacks on ciphertext images, the algorithm can still obtain plaintext information after decryption of ciphertext images. It is effective to show that the algorithm is feasible.

5 In conclusion

This paper proposes a bit-level image encryption algorithm based on BP neural network and Gray code. In the permutation, the Gray code is used for the bit-level permutation operation. In the diffusion, the bit-level reverse-order output is first adopted, and then the chaotic map is outputted through the BP neural network model for the divergence xor operation. After a lot of experimental tests, the algorithm can be used for image encryption and it works well.

Acknowledgments This research is supported by the National Natural Science Foundation of China (No: 61672124), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund (No: MMJJ20170203), Liaoning Province Science and Technology Innovation Leading Talents Program Project (No: XLYC1802013), Key R&D Projects of Liaoning Province (No: 2019020105-JH2/103), Jinan City '20 universities' Funding Projects Introducing Innovation Team Program (No: 2019GXRC031).

References

1. Ahmad M, Alam MZ et al Cryptanalysis of an image encryption algorithm based on PWLCM and inertial delayed neural network. J Intell Fuzzy Syst Appl Eng Technol 34(3):1323–1332
2. Alawida M, Samsudin A, Sen TJ et al (2019) A new hybrid digital chaotic system with applications in image encryption. Signal Process 160:45–58
3. Gan ZH, Chai XL, Yuan K et al (2018) A novel image encryption algorithm based on LFT based S-boxes and chaos. Multimed Tools Appl 77(7):8759–8783
4. Gao H, Zeng W (2019) Image compression and encryption based on wavelet transform and chaos. Comput Opt 43(2):258–263
5. Han CY (2019) An image encryption algorithm based on modified logistic chaotic map. Optik 181:779–785
6. Kumar M, Iqbal A, Kumar P (2016) A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Process 125:187–202
7. Liu HJ, Kadir A, Sun XB et al (2018) Chaos based adaptive double-image encryption scheme using hash function and S-boxes. Multimed Tools Appl 77(1):1391–1407
8. Lv XP, Liao XF, Yang B (2018) Bit-level plane image encryption based on coupled map lattice with time-varying delay. Mod Phys Lett B 32(10):1850124
9. Maddodi G, Awad A, Awad D, Awad M, Lee B (2018) A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding. Multimed Tools Appl 77(19):24701–24725
10. May RM (1976) Simple mathematical models with very complicated dynamics. Nature 261(5560):459–467
11. Pak C, An K, Jang P, Kim J, Kim S (2019) A novel bit-level color image encryption using improved 1D chaotic map. Multimed Tools Appl 78(9):12027–12042
12. Ratnavelu K, Kalpana M, Balasubramaniam P, Wong K, Raveendran P (2017) Image encryption method based on chaotic fuzzy cellular neural networks. Signal Process 140:87–96
13. Sokouti M, Sokouti B (2018) A PRISMA-compliant systematic review and analysis on color image encryption using DNA properties. Comput Sci Rev 29:14–20
14. Sun SL (2018) A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. IEEE Photon J 10(2):7201714
15. Tang Y, Wang ZD, Fang JA (2010) Image encryption using chaotic coupled map lattices with time-varying delays. Commun Nonlinear Sci Numer Simul 15(9):2456–2468
16. Teng L, Wang XY (2012) A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive. Opt Commun 285(20):4048–4054
17. Wang XY, Gao S (2020) Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Inf Sci 507:16–36
18. Wang XY, Gao S (2020) Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Inf Sci 539:195–214
19. Wang XY, Jin CQ (2012) Image encryption using game of life permutation and PWLCM chaotic system. Opt Commun 285(4):412–417
20. Wang X, Li Z (2019) A color image encryption algorithm based on Hopfield chaotic neural network. Opt Lasers Eng 115:107–118
21. Wang XY, Wang MJ (2007) Hyperchaotic Lorenz system. Acta Phys Sin 56(9):5136–5141
22. Wang XY, Feng L, Zhao HY (2019) Fast image encryption algorithm based on parallel computing system. Inf Sci 486:340–358
23. Wang XY, Zhao HY, Feng L et al (2019) High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices. Opt Lasers Eng 122:225–238
24. Wang XY, Zhao HY, Wang MX (2019) A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices. Opt Laser Technol 115:42–57
25. Wang XY, Zhang JJ, Cao GH (2019) An image encryption algorithm based on ZigZag transform and LL compound chaotic system. Opt Laser Technol 119:105581
26. Wang XY, Zhang JJ, Zhang FC, Cao GH (2019) New chaotical image encryption algorithm based on fisher–Yatess scrambling and DNA coding. Chin Phys B 28(4):040504
27. Wei T, Lin P, Wang Y, Wang L (2019) Stability of stochastic impulsive reaction–diffusion neural networks with S-type distributed delays and its application to image encryption. Neural Netw 116:35–45
28. Wu JH, Liao XF, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Process 141:109–124
29. Wu XJ, Kurths J, Kan HB (2018) A robust and lossless DNA encryption scheme for color images. Multimed Tools Appl 77(10):12349–12376
30. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25

31. Younas I, Khan M (2018) A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System. Entropy 20(12):913
32. Zhang YQ, Wang XY (2015) A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 26:10–20
33. Zhang YS, Xiao D (2014) An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun Nonlinear Sci Numer Simul 19(1):74–82
34. Zhang YQ, Wang XY, Liu J, Chi ZL (2016) An image encryption scheme based on the MLNCML system using DNA sequences. Opt Lasers Eng 82:95–103
35. Zhang LM, Sun KH, Liu WH, He SB (2017) A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations. Chin Phys B 26(10):100504
36. Zhang XP, Guo R, Chen HW, Zhao ZM, Wang JY (2018) Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes. Chin Phys B 27(8):080701
37. Zhou NR, Chen WW, Yan XY et al (2018) Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Inf Process 17(6):137

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.