Application of quantum genetic algorithm in high noise laser image security*

MAN Zhenlong[1,2], LI Jinqing[1,2], DI Xiaoqiang[1,2,3]**, and MU Yining[4]**

1. School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China

2. Jilin Province Key Laboratory of Network and Information Security, Changchun 130022, China

3. Information Center of Changchun University of Science and Technology, Changchun 130022, China

4. School of Science, Changchun University of Science and Technology, Changchun 130022, China

(Received 30 April 2021; Revised 19 July 2021)

Aiming at the security problem of range gated laser imaging in high noise background, a range gated laser image encryption scheme based on the quantum genetic algorithm (QGA) is proposed. Due to the fuzziness of the laser image itself, the randomness and security of the key become more and more important in encryption. In this paper, the chaotic sequence is used as the parent chromosome of the QGA, and the random number satisfying the encryption algorithm is obtained by an iterative genetic algorithm. To further improve the security of laser images, some random pixels are stochastically inserted around the laser image before scrambling. These random pixels are scrambled together with the image. Finally, an adaptive diffusion method is designed to completely change the original statistical information of the image. Experimental simulation and performance analysis show that the scheme has high security.

Document code: A **Article ID:** 1673-1905(2022)01-0059-6

DOI https://doi.org/10.1007/s11801-022-1070-5

Laser is a brand-new subject developed in the 1960s, and laser imaging technology has also emerged with the development of laser technology[1]. Range-gated laser imaging uses the current mature microchannel plate (MCP) and charge-coupled device (CCD) technology to intuitively obtain rich target shape or basic structural information, which can effectively suppress back scattered noise interference as well as identify the target and its key parts, especially distance selection[2]. Laser imaging technology has irreplaceable advantages and important research value in military applications. Therefore, the security of laser images has been widely concerned by researchers[3].

Because the image has the characteristics of high redundancy, large capacity and strong correlation between adjacent pixels, the traditional text encryption scheme cannot guarantee the security of the image[4]. Therefore, researchers have proposed many image encryption schemes based on chaos[5]. Chaotic mapping is very suitable for key generation. One of the reasons is its randomness, unpredictability and extreme sensitivity to initial values and parameters. On the other hand, they are deterministic and easy to reproduce[6]. However, it is found that only the pseudo-random number generated by chaotic system is not safe. Therefore, in order to improve the security and randomness of key, many scholars combine chaotic system with other methods, such as breadth first search[7], edge encryption, elliptic curve[8], etc. In this paper, chaotic system and quantum genetic algorithm (QGA) are combined to generate encryption key with good randomness. QGA is the combination of quantum computing and traditional genetic algorithm. It is a new probabilistic evolutionary algorithm developed in the late 1990s. NARAYANAN et al[9] first proposed the concept of quantum derived genetic algorithm QGA. Then, HAN et al[10] proposed a QGA based on the superposition of qubits and quantum states. In addition, it is applied to knapsack problem and achieves better results than traditional genetic algorithm. Therefore, the algorithm has rapidly become a research hotspot at home and abroad. Researchers have made a series of improvement and application research on QGA. We start from a new point of view, using chaotic sequence as parent chromosome in QGA. Through quantum phase rotation and mutation, the encryption key with good randomness is obtained.

The existing image encryption schemes are mainly composed of scrambling stage and diffusion stage, and the design of scrambling algorithm and diffusion algorithm has always been the focus of researchers[11].

Scrambling stage is to change the position of image pixels, which will lead to visual confusion. Most authors use scrambling models to encrypt/decrypt images[12-14], but the scrambling effect of these schemes is not ideal. To solve this problem, this paper designs a novel scrambling

* This work has been supported by the National Key Research and Development Projects (No.2018YFB1800303), the Natural Science Foundation of Jilin Province (No.20190201188JC), and the Research on Teaching Reform of Higher Education in Jilin Province (No.JLLG685520190725093004).

** E-mails: lijinqing@cust.edu.cn; dixiaoqiang@cust.edu.cn

method, adding random pixels around the image before scrambling. These random pixels are generated in different ways each time. Even the encryptor cannot determine these random numbers. Then the inserted pixels and the original image pixels are diffused together, which not only has no effect on the decryption effect, but also effectively improves the security of the encryption system.

Diffusion stage is to change the pixel value of the image, and spread among different pixels. In recent years, researchers have designed many excellent diffusion algorithms[15]. Although these algorithms have good performance, they cannot flexibly adjust the diffusion operation of the algorithm for different images. Aiming at these problems, this paper designs an adaptive image diffusion scheme, which can adaptively adjust the diffusion operation according to different images, so that the encryption algorithm is more flexible and always maintains high security.

Before introducing the encryption algorithm, we first understand the preparatory work needed.

The three-dimensional Lorenz chaotic[16] frameworks is described by

$$\begin{cases} \dfrac{\mathrm{d}x}{\mathrm{d}t} = \alpha(y-x) \\ \dfrac{\mathrm{d}y}{\mathrm{d}t} = \beta x - y - xz \\ \dfrac{\mathrm{d}z}{\mathrm{d}t} = xy - \gamma z \end{cases}, \tag{1}$$

where α, β, γ are the constant real numbers. When α=3, β=5, γ=10, the system is chaotic and its Lyapunov exponents are λ_1=0.03, λ_2=−0.01, λ_3=−7.78. There exists a positive Lyapunov exponent. Thus, the system has chaotic characteristics.

QGA is an intelligent optimization algorithm combining quantum computing with genetic algorithm. It introduces quantum concepts such as quantum state, quantum gate, quantum state characteristics, and probability amplitude into the genetic algorithm.

$$\begin{cases} \boldsymbol{P}_i = \left[\begin{vmatrix} \cos\theta_{i1} \\ \sin\theta_{i1} \end{vmatrix} \begin{vmatrix} \cos\theta_{i2} \\ \sin\theta_{i2} \end{vmatrix} \ldots \begin{vmatrix} \cos\theta_{ik} \\ \sin\theta_{ik} \end{vmatrix} \right] \\ \theta_{ij} = 2\pi \times rand, i = 1,2,3,...,n; j = 1,2,3,...,k \end{cases}, \tag{2}$$

where θ is the phase of qubits, n is the number of chromosomes, k is the number of qubits, and *rand* is a random number in the range of [0,1].

The key generation method is as follows.

Step 1: Iterate chaotic system (1) to generate three random sequences x, y, z.

Step 2: Divide the random sequence x, y and z into two parts, which are used as the parent chromosome of QGA.

Step 3: The parent chromosome is transformed into solution space.

Step 4: In the input algorithm, qubit phase rotation and qubit phase mutation are performed.

Step 5: The new quantum chromosome is obtained, and the pseudo-random $S1$, $S2$, $S3$, $S4$ are obtained by solution space transformation.

A laser image encryption algorithm based on QGA security key is proposed. In this algorithm, the chaotic sequence generated by the low dimensional chaotic system is input into QGA as the initial parent chromosome, and the mutated chromosome is obtained by the operation of qubit phase rotation and qubit phase mutation. Finally, the new pseudo-random number is applied to our image encryption algorithm, and the experimental analysis shows that the scheme has high security. Fig.1 is a schematic diagram of the encryption algorithm.

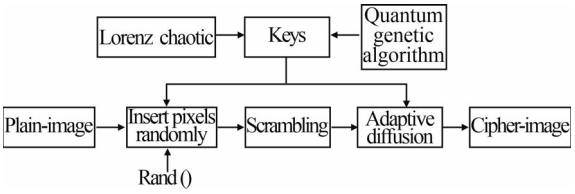


Fig.1 Block diagram of encryption process

Step 1: Take the laser image of size M×N as the plain-image P.

Step 2: The pseudo-random number is generated by Eq.(3) and mapped to the value in the range of 0—256:

$$\begin{cases} IN = \mathrm{rand}(50) \\ IN_1 = \mathrm{floor}(\mathrm{mod}(IN \times 10^{15}, 256)) \end{cases}, \tag{3}$$

where rand () is to generate random number, floor () is to round down, and mod () is to take module operation.

Step 3: Insert the random number in step 2 around the plain-image to get a new image IN_P, as shown in Fig.2 (suppose the size of plain-image is 4×4).

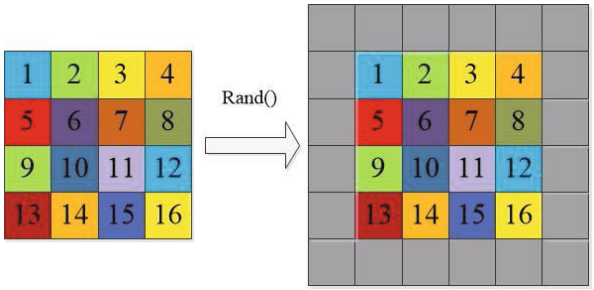


Fig.2 Random insert pixel diagram

Step 4: Map the random sequence $S1$ to S_x through Eq.(4), and then eliminate the duplicate data in S_x to get the positioning coordinates (Loc_x, Loc_y):

$$\begin{cases} S_x = \mathrm{mod}(S1 \times 10^{15}, M+2) \\ Loc_x = \mathrm{uniqe}(S_x(1:\dfrac{M \times N}{2})) \\ Loc_x(\mathrm{find}(Loc_x == 0)) = [] \\ Loc_y = \mathrm{uniqe}(S_x(1:\dfrac{M \times N}{2})) \\ Loc_y(\mathrm{find}(Loc_y == 0)) = [] \end{cases}, \tag{4}$$

where unique () means to remove the duplicate data in the matrix, find () means the position of the non-zero elements in the return vector, and [] means to leave the 0 elements empty.

Step 5: The pixels in the image are exchanged with the pixels controlled by the positioning coordinates in the

order from left to right and from top to bottom, as shown as

$$P_s=\begin{cases}\partial = IN_p(i,j)\\ IN_p(i,j)=IN_p(Loc_x(i),Loc_y(j)),\\ IN_p(Loc_x(i),Loc_y(j))=\partial\end{cases} \tag{5}$$

where ∂ is the intermediate variable, i=1, 2, 3,…, 258, j=1, 2, 3,…, 258.

Step 6: For pseudo-random sequences $S2$, $S3$ and $S4$, the diffusion keys S_y, S_z and S_w are obtained as shown as

$$\begin{cases}S_y=\mathrm{mod}(S2\times10^{15},256)\\ S_z=\mathrm{mod}(S3\times10^{15},256).\\ S_w=\mathrm{mod}(S4\times10^{15},256)\end{cases} \tag{6}$$

Step 7: Further, the scrambled image P_S carries on the dynamic adaptive diffusion to obtain the final cipher-image P_d.

The diffusion diagram is shown in Fig.3 and Eq.(7) as follows

$$\begin{cases}P_s(\tau)=\mathrm{bitxor}(S_y(\tau),P_s-\mu)\\ P_d(\tau+1)=\mathrm{bitxor}(\mathrm{bitxor}(P_d(\tau),P_s(\tau+1)),S_z(\tau+1)),\\ P_d(\tau-1)=\mathrm{bitxor}(\mathrm{bitxor}(P_d(\tau),P_s(\tau-1)),S_z(\tau-1))\end{cases} \tag{7}$$

where μ and τ are user control parameters.

Since the algorithm is a symmetric encryption algorithm, the decryption process is the inverse of the encryption process.

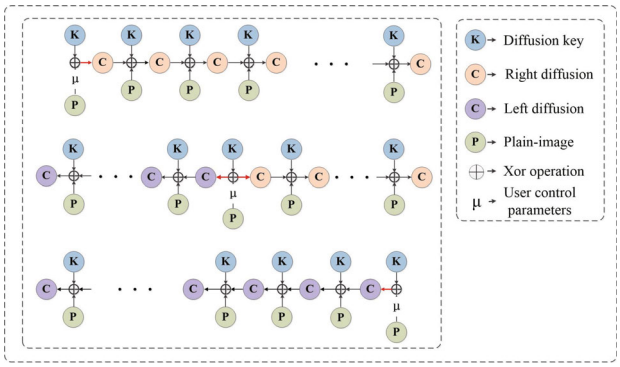


Fig.3 Dynamic adaptive diffusion diagram

In this section, we will discuss the performance of the proposed algorithm. We choose 256×256 gated laser images "Triangular prism" and "people" as test images, and Fig.4 shows the effect of encryption and decryption.

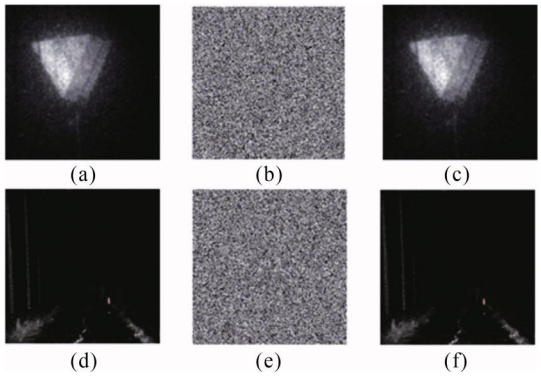


Fig.4 Image encryption and decryption results: (a) (d) Original images; (b) (e) Encrypted images; (c) (f) Decrypted images

The key space of an excellent encryption algorithm should be greater than 2^{100} to resist violent attacks. The initial values and parameters of the chaotic system are x, y, z, α, β, γ. The parameters of the QGA are initial population size, quantum number of a chromosome, turning step, mutation probability, and iteration time. Because the precision of initial value and parameters of a chaotic system is 10^{-16}, the key space is $(10^{-16})^6>2^{192}$, so the key space is large enough to resist all kinds of violent attacks.

A secure cryptosystem should be sensitive to the key. A slight change in the encryption key will result in a completely different ciphertext image. Similarly, a slight change in the decryption key will lead to the failure to decrypt the correct plain-image. Taking 256×256 "Triangular prism" image as an example, if the 16th digit value after the decimal point in the initial values x, y and z of the chaotic system is changed respectively, as shown in Fig.5(c)—(e), the wrong key cannot decrypt the original image normally. This demonstrates that the key of our algorithm has high sensitivity.

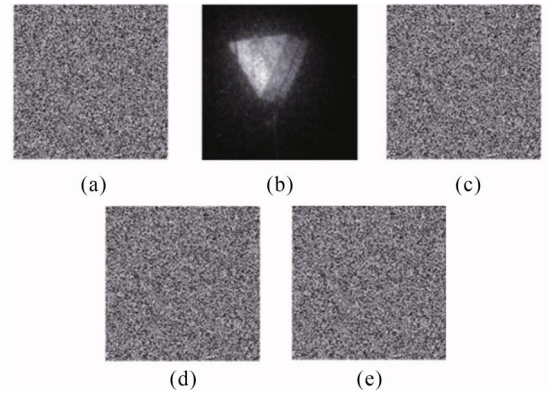


Fig.5 Key sensitivity results: (a) Cipher-image; (b) Decryption image using the correct decryption key; (c) Incorrect decryption using x+10^{-16}; (d) Incorrect decryption using y+10^{-16}; (e) Incorrect decryption using z+10^{-16}

Histogram analysis is an important aspect to reflect the frequency distribution of image gray value. A secure encryption scheme should generate images with a uniform histogram to improve the ability to resist statistical analysis. This paper analyzes the histogram of two plain-images and their cipher-images. Fig.6 shows the "Triangular prism" and "people" images and their histograms. It can be observed that the histogram distribution of the encrypted image is average, which shows that the algorithm can resist any statistical attack.

Information entropy is an important parameter reflecting the randomness of information. The calculation method is as follows

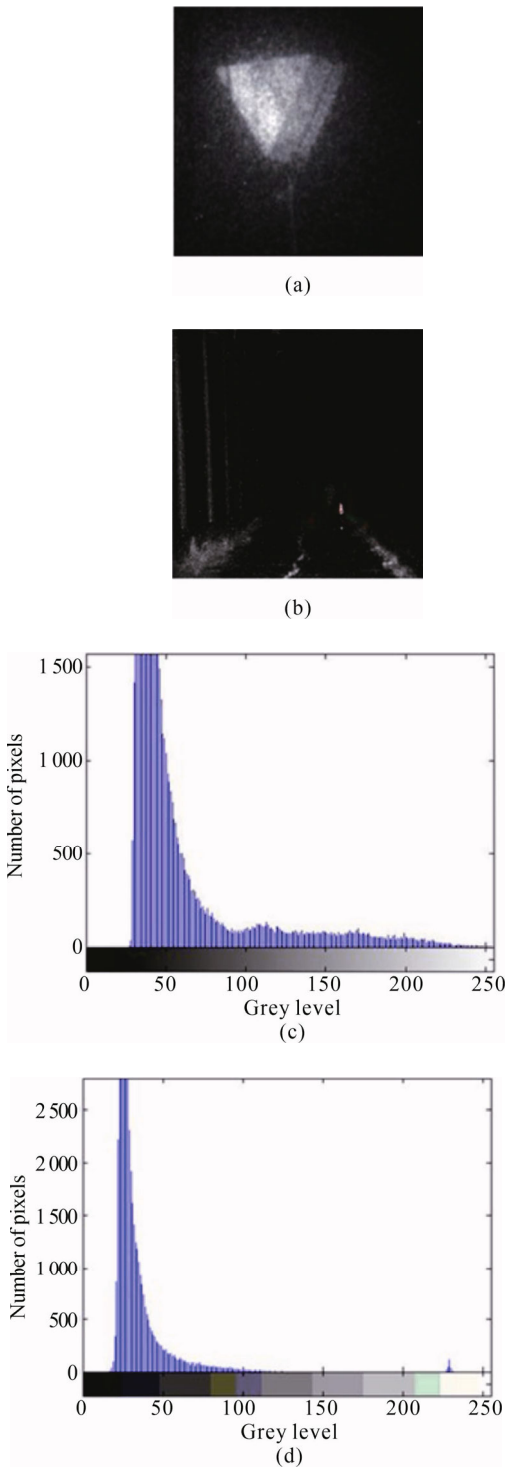
$$H(S,L)=\sum_{i=0}^{2^L-1}p(s_i)\log_2\frac{1}{p(s_i)}, \tag{8}$$

where $S=[s_i]_{2L}$, $p(s_i)$ is the probability of s_i. In our experiment, we let L=8, so $H(S, 8)$=8. In theory, the closer the information entropy is to 8, the smaller the possibility

of information leakage. In parallel, we also compare the entropy value of this scheme with other similar algorithms. The results show that our entropy value is closer to the theoretical value than that of similar literature, which further proves that this scheme has certain advantages.

Tab.1 Information entropy

	"Triangular prism"	"People"	Ref.[14]	Ref.[15]
Cipher-image	7.998 1	7.997 5	7.997 1	7.997 2



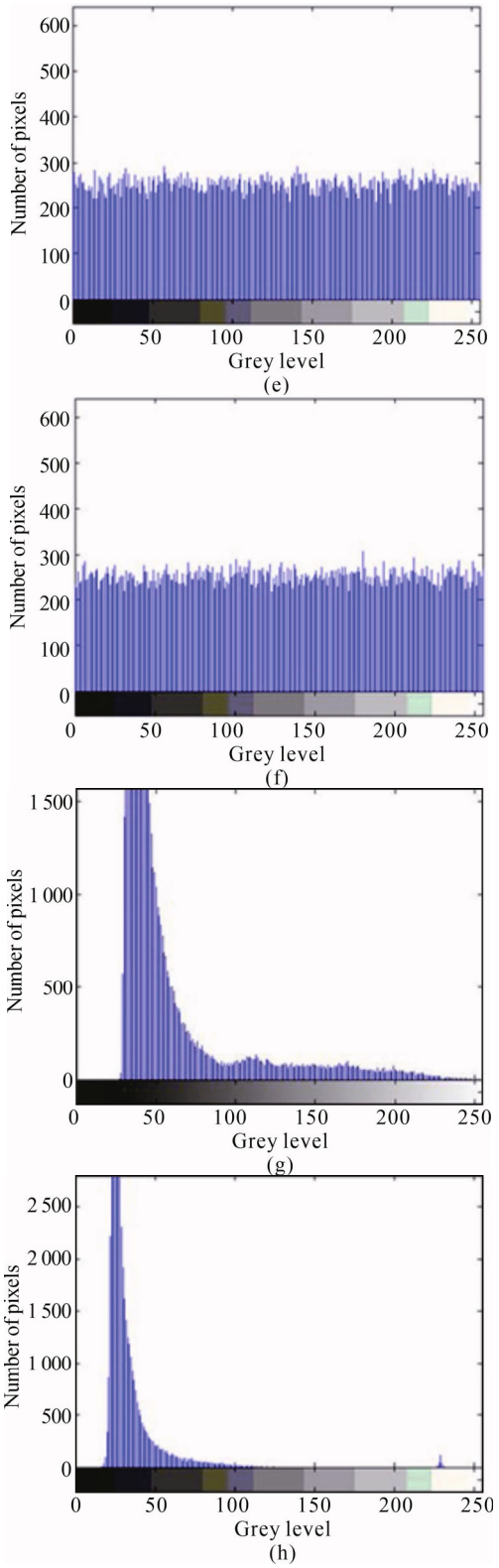


Fig.6 Histogram results: (a) (b) Plain-images; (c) (d) Plain-image histograms; (e) (f) Encrypted images; (g) (h) Encrypted image histograms

Correlation analysis is a means to calculate the similarity between two data. In an image, the color intensity of an adjacent pixel is nearly the same. Therefore, there is a high degree of similarity between the two pixels, and the correlation coefficient is high. However, a powerful

and efficient encryption algorithm should make the ciphertext image have a lower correlation coefficient as far as possible. In this paper, 4 000-pixel samples are assumed to calculate the correlation coefficients in horizontal, vertical, and diagonal directions. The function for calculating the correlation coefficient is shown as

$$\begin{cases} r_{xy} = \mathrm{cov}(x,y)/\sqrt{D(x)D(y)} \\ E(x) = \dfrac{1}{S}\sum_{i=1}^{S} x_i \\ D(x) = \dfrac{1}{S}\sum_{i=1}^{S}(x_i - E(x))^2 \\ \mathrm{cov}(x,y) = \dfrac{1}{S}\sum_{i=1}^{S}(x_i - E(x))(y_i - E(y)) \end{cases}, \tag{9}$$

where x and y represent the gray values of two adjacent pixels, respectively. According to the analysis of Fig.7, the neighborhood correlation coefficient of cipher-image is lower than that of plain-image. It can be shown in Tab.2 that the correlation coefficient of cipher-image is significantly reduced, which is approximately zero, and the correlation is lower than the values of literature. This further proves that our algorithm can effectively resist statistical attacks.

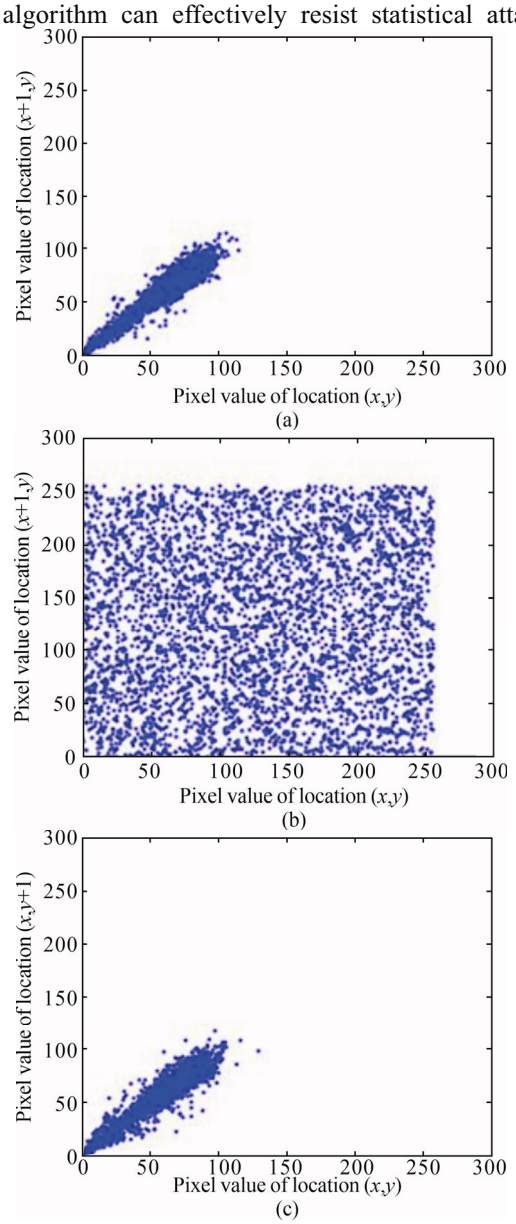


Fig.7 Pixel correlation coefficient analysis: (a) Horizontal adjacent pixel correlation of the plain-image; (b) Horizontal adjacent pixel correlation of the cipher-image; (c) Vertical adjacent pixel correlation of the plain-image; (d) Vertical adjacent pixel correlation of the green component of the cipher-image; (e) Diagonal adjacent pixel correlation of the blue component of the plain-image; (f) Diagonal adjacent pixel correlation of the cipher-image

Tab.2 Correlation coefficients of the cipher-images

Direction	Horizontal	Vertical	Diagonal
"Triangular prism"	0.000 2	0.004 2	−0.002 4
"people"	0.006 4	0.000 9	0.008 1
Ref.[14]	0.005 8	0.027 5	0.004 7
Ref.[15]	−0.000 3	−0.001 6	0.002 2

The difference between plaintext image and cipher image can be measured by mean square error (*MSE*). We use peak signal-to-noise ratio (*PSNR*) to detect the quality of cipher image. The details are as follows

$$\begin{cases} MSE = \dfrac{\sum_i \sum_j (P(i,j) - C(i,j))^2}{T} \times 100\% \\ PSNR = 10 \log_{10}(\dfrac{I_{\max}^2}{MSE}) \end{cases}, \tag{10}$$

where T represents the number of pixels in the image, $P(i, j)$ is the value of the pixels of plain-image, $C(i, j)$ is the pixel value of the encrypted image, and $I_{\max}$ is the maximum pixel value of the encrypted image. Although the laser image has higher noise, it can still get lower *PSNR* value after encryption, as shown in Tab.3. By comparing with ordinary digital image, we find that our algorithm has a better effect for laser image encryption.

Tab.3 *MSE* and *PSNR* for the encryption

	"Triangular prism"	"people"	Ref.[4]
MSE	11 782	15 026	11 385
PSNR	7.418 5	6.362 4	7.567 4

Based on the characteristics of gated laser images, a secure random number generation scheme is designed, which combines QGA with chaotic system reasonably. A novel scrambling and diffusion algorithm is proposed to improve the security of the image. Next, we will deeply study the security of gated laser image, and consider hiding the laser image information in other multimedia media, which can improve the image security in the process of image transmission.

Statements and Declarations

The authors declare that there are no conflicts of interest related to this article.

References

[1] OSAWA H, YAMAMOTO H. Present and future status of flexible spectral imaging color enhancement and blue laser imaging technology[J]. Digestive endoscopy, 2014, 26(Suppl. 1)：105-115.

[2] GHLER B, LUTZMANN P, ANSTETT G. 3D imaging with range gated laser systems using speckle reduction techniques to improve the depth accuracy[J]. Proceedings of SPIE-electro-optical and infrared systems：technology and applications V, 2008, 7113：711307.

[3] STEINVALL O, ANDERSSON P, ELMQVIST M, et al. Overview of range gated imaging at FOI[C]//Infrared Technology and Applications XXXIII, April 9-13, 2007, Orlando, Florida, USA. Bellingham：SPIE, 2007：654216.

[4] MAN Z, LI J, DI X, et al. An image segmentation encryption algorithm based on hybrid chaotic system[J]. IEEE access, 2019, 7：103047-103058.

[5] ZHANG Y. The fast image encryption algorithm based on lifting scheme and chaos[J]. Information sciences, 2020, 520：177-194.

[6] ISMAIL S M, SAID L A, RADWAN A G, et al. A novel image encryption system merging fractional-order edge detection and generalized chaotic maps[J]. Signal processing, 2020, 167：107280.

[7] YIN Q, WANG C. A new chaotic image encryption scheme using breadth-first search and dynamic diffusion[J]. International journal of bifurcation and chaos, 2018, 28(04)：1850047.

[8] EL-LATIF A A A, NIU X. A hybrid chaotic system and cyclic elliptic curve for image encryption[J]. AEU-international journal of electronics and communications, 2013, 67(2)：136-143.

[9] NARAYANAN A, MOORE M. Quantum-inspired genetic algorithms[C]//Proceedings of IEEE International Conference on Evolutionary Computation, May 20-22, 1996, Nagoya, Japan. New York：IEEE, 1996：61.

[10] HAN K H, KIM J H. Genetic quantum algorithm and its application to combinatorial optimization problem[C]// Proceedings of the 2000 Congress on Evolutionary Computation, July 16-19, 2000, La Jolla, CA, USA. New York：IEEE, 2000：1354-1360.

[11] WU J, LIAO X, YANG B. Image encryption using 2D Hénon-Sine map and DNA approach[J]. Signal processing, 2018, 153：11-23.

[12] GUESMI R, FARAH M B. A new efficient medical image cipher based on hybrid chaotic map and DNA code[J]. Multimedia tools and applications, 2021, 80(2)：1925-1944.

[13] ZHOU Y, LI C, LI W, et al. Image encryption algorithm with circle index table scrambling and partition diffusion[J]. Nonlinear dynamics, 2021, 103(2)：2403-2601.

[14] MAN Z, LI J, DI X. Image encryption algorithm based on dual fingerprint control[C]//2020 IEEE 5th International Conference on Signal and Image Processing (ICSIP), October 23-25, 2020, Southeast University, Nanjing, China. New York：IEEE, 2020：236.

[15] ZHU S, ZHU C. Secure image encryption algorithm based on hyperchaos and dynamic DNA coding[J]. Entropy, 2020, 22(7)：772.

[16] RAKHEJA P, VIG R, SINGH P. Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition[J]. Optical and quantum electronics, 2020, 52(2)：103.