Range-gated laser image compression and encryption scheme based on bidirectional diffusion*

LI Jinqing (李锦青)[1,2]**, **SHENG Yaohui** (盛耀辉)[1,2], **DI Xiaoqiang** (底晓强)[1,2,3], and **MU Yining** (母一宁)[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 7 January 2021)

The existing image encryption schemes are not suitable for the secure transmission of large amounts of data in range-gated laser imaging under high noise background. Aiming at this problem, a range-gated laser imaging image compression and encryption method based on bidirectional diffusion is proposed. The image data collected from the range-gated laser imaging source is sparsely represented by the discrete wavelet transform. Arnold chaotic system is used to scramble the sparse matrix, and then the measurement matrix is constructed by the quantum cellular neural network (QCNN) to compress the image. In addition, the random sequence generated by QCNN hyperchaotic system is used to carry out "bidirectional diffusion" operation on the compression result, so as to realize the security encryption of image data. The comparative analysis of the security encryption performance of different compression ratios shows that the histogram sample standard of the encrypted image can reach about 10, and the information entropy value is more than 7.99, which indicates that the encryption scheme effectively hides the plaintext information of the original image. When the encrypted image is attacked by different degrees of noise, this method can still reconstruct the image through the effective decryption process. The experimental results show that this method realizes the secure compression and encryption of gated-laser imaging image data, and effectively ensures the security of data while reducing the amount of channel transmission data.

Document code: A **Article ID:** 1673-1905(2021)10-0630-6

DOI https://doi.org/10.1007/s11801-021-1003-8

Laser active imaging is an imaging method using the laser as the light source. It is an imaging method that laser beams with specific parameters are emitted by the laser transmitting device to irradiate the target object, and the laser echo reflected by the target is received by the receiving system to obtain the target image[1]. Laser active imaging system has more advantages than passive imaging system, such as not relying on external illumination source, not limited by night, long operating distance, and can obtain three-dimensional image of the target. Range-gated laser imaging is an important research branch of laser active imaging, which solves the problem of backward diffusion of medium in laser active imaging[2,3]. At present, range-gated laser imaging technology is widely used and plays an important role in space, surveying and mapping, remote sensing, night vision security, and airborne imaging[4]. In particular, range-gated laser imaging technology has irreplaceable advantages and important research value in the field of military applications[5].

With the development of laser technology, people pay more and more attention to the key technologies of gated imaging. In 2017, Guan et al[6] designed a 3D imaging system for underwater targets, which can generate high-precision 3D images of targets. In 2019, Lv et al[7] aimed at the problem of rapid attenuation of light wave in water, in the range-gated laser imaging system, blue-green laser with high intensity, high monochromaticity, and high transmittance was used as the light source, and the experiment shows that the method has a longer imaging distance.

With the rapid development of Internet communication technology, various types of image data obtained by gated laser imaging technology are subject to various forms of security threats. The problem of information security of laser imaging data has attracted wide atten-

* 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-mail: lijinqing@cust.edu.cn

tion from researchers. Image encryption is an important It is a method to reconstruct the original image into a noise-like image. The encrypted image can effectively hide the useful information of the original image, and the attacker cannot crack the content of the original data through the encrypted image analysis. Therefore, the introduction of image encryption technology into the field of laser imaging will become an inevitable trend.

Image encryption technology has been widely used in online banking, medical imaging, military communications, satellite security, enterprise communications, and other fields. In 2019, Chen et al[8] proposed a medical image encryption scheme based on discrete wavelet transform (DWT) and five-dimensional hyperchaotic system. The medical image is divided into regions of interest (ROI) and background regions, and the ROI is encrypted by discrete wavelet transform and chaotic scrambling and diffusion process. In 2019, Man et al[9] proposed an image segmentation and encryption algorithm based on a hybrid chaotic system is proposed. The key pool is obtained by iterative QCNN. Secondly, the key for image segmentation, scrambling, and diffusion is obtained from the key pool. Then, the original image is divided into two blocks by chaotic segmentation method and scrambled by intra block and inter block pixel exchange. In addition, the cipher image is obtained by static and dynamic diffusion of the two blocks.

However, different from ordinary digital images, the amount of image data collected by gated laser imaging is large[10]. In the case of external environment interference, the laser active imaging system is difficult to obtain a clear image[11], and sometimes the output image needs to be observed in real-time. The increasing amount of image transmission takes up a lot of transmission broadband, which brings great pressure to real-time transmission. Therefore, the traditional digital image encryption method is not suitable for gated laser imaging security encryption.

In order to solve the problem of safe and efficient transmission of range-gated laser imaging system output image in the communication link, an image encryption algorithm based on compressed sensing and bidirectional diffusion is proposed. The scheme realizes the compression and encryption of the laser gated image, reduces the size of the encrypted image file, and the encrypted image does not contain any information of the original image. Experiments show that the scheme can resist statistical analysis and noise attacks. The decryption and reconstruction of encrypted compressed image are realized under noise background, and the original image content of the laser gated image is restored.

The range-gated laser imaging system is mainly composed of three parts: transmitting system, control system, and receiving system[12]. Because of the high brightness, good directivity, and high monochromaticity of laser, laser is used as the irradiation source in the emission system. The control system is mainly used to control whether the gate in the receiving system is open or not, technical means to protect the image information security. and the receiving system images according to the reflected light from the target. As shown in Fig.1, the transmitting system emits laser signal and reflects the signal after reaching the target surface. When the reflected signal reaches the receiving system, the control system makes the gate of the receiving system open, and in other cases, the gate is always closed. In this way, the image signal received by the system is only the reflection signal of the target, which is conducive to improving the image quality.

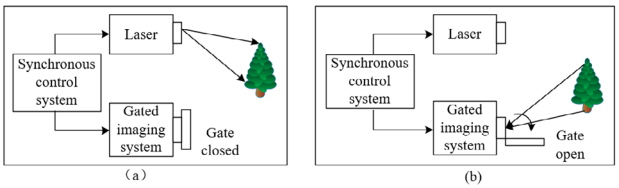

Fig.1 Schematic diagram of range-gated laser imaging principle: (a) Gate closed; (b) Gate open

Compressed sensing is a kind of sampling and reconstruction technology, which can realize image sampling, compression, and encryption at the same time. Therefore, it has received more and more attention and has been widely studied in the industry. The implementation of compressed sensing theory includes three key parts: sparse representation, coefficient measurement, and signal reconstruction[13,14]. The process is shown in Fig.2.

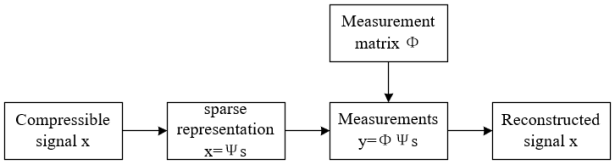

Fig.2 Process diagram of compressed sensing

The image security encryption scheme is mainly based on the scrambling-diffusion structure, as shown in Fig.3.

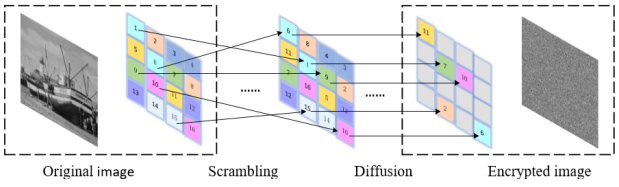

Fig.3 Scrambling-diffusion image security encryption structure

In this paper, QCNN and Arnold transform hyperchaotic systems are used to generate the key[15]. Arnold transform is a digital image scrambling technology, which exchanges the positions of each pixel in the image, and each pixel is uniquely changed into another point. The scrambling process is shown in Fig.4.

Arnold transform can be regarded as the process of stretching, compressing, folding, and stitching images. It rearranges the points in the discrete digital image matrix

to make the original meaningful image become a meaningless image, so as to achieve the effect of encryption.

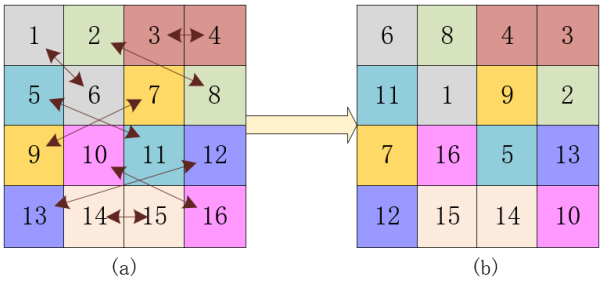

Fig.4 Arnold scrambling process: (a) Original image; (b) Scrambling image

Quantum dots and quantum cellular automata are new nano electronic devices that transmit information through Coulomb interaction. Compared with traditional techniques, quantum cellular automata have the advantages of ultra-high integration, ultra-low power consumption, and leadless integration. In recent years, scholars at home and abroad have constructed QCNN on the basis of Schrodinger equation by using the structure of cellular neural network and quantum cellular automata. Due to the quantum interaction between quantum dots, QCNN can obtain complex linear dynamic characteristics from the polarizability and quantum phase of each quantum cellular automata, which can be used to construct nano scale hyperchaotic oscillators. The QCNN coupled with two elements can be described by the following differential equations:

$$\begin{cases} \dot{g}_1 = -2a_1\sqrt{1-g_1^2}\sin h_1 \\ \dot{h}_1 = \left(-b_1\left(g_1-g_2\right)+2a_1\cos h_1\right)/\left(\sqrt{1-g_1^2}\right) \\ \dot{g}_2 = -2a_2\sqrt{1-g_2^2}\sin h_2 \\ \dot{h}_2 = \left(-b_2\left(g_2-g_1\right)+2a_2g_2\cos h_2\right)/\left(\sqrt{1-g_2^2}\right) \end{cases}, \quad (1)$$

where g_1 and g_2 are the polarizability, h_1 and h_2 are the quantum phases, a_1 and a_2 are the proportional coefficients of energy between the points in each element, b_1 and b_2 are the weighted influence factors of polarizability difference between adjacent cells. When a_1=a_2=0.28, b_1=0.7, b_2=0.3, the system is in chaotic state. Four pseudo-random sequences G_1, H_1, G_2, H_2 are generated by iterative QCNN hyperchaotic system. In order to eliminate the instantaneous effect, the first t term of the sequence is discarded. The key stream Q_1, Q_2, Q_3, Q_4 can be expressed by:

$$\begin{cases} Q_1 = G_1\left(t+1:N\times N+t\right) \\ Q_2 = H_1\left(t+1:N\times N+t\right) \\ Q_3 = G_2\left(t+1:N\times N+t\right) \\ Q_4 = H_2\left(t+1:N\times N+t\right) \end{cases}. \quad (2)$$

Considering the low resolution and low definition of range-gated imaging, in order to meet the needs of safe and efficient storage and transmission of laser gated image, we propose an image encryption scheme based on compressed sensing, chaotic scrambling, and bidirectional diffusion. The scheme realizes the secure compression and encryption of the range-gated laser image, and ensures the safe and efficient transmission of the image in the channel. The structure of the security encryption system is shown in Fig.5.

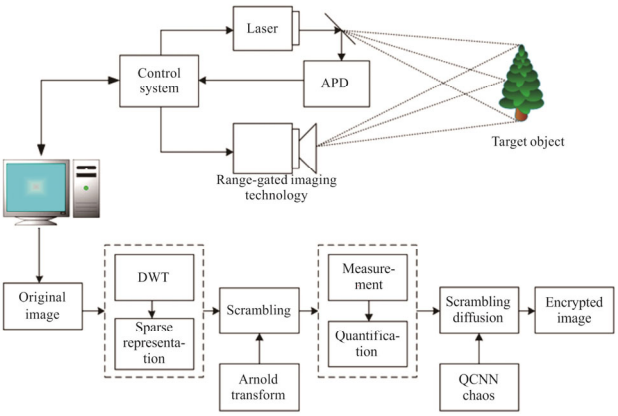

Fig.5 Block diagram of the range-gated laser image security encryption scheme

Firstly, an N×N range-laser gated image $\boldsymbol{P}$ is selected to perform DWT[16] for the original image $\boldsymbol{P}$, which is sparse represented by DWT to make it compressible. The resulting sparse matrix is denoted as $\boldsymbol{SM}$.

$$\boldsymbol{SM}=\mathrm{DWT}(\boldsymbol{P}), \quad (3)$$

where DWT () represents discrete wavelet transform.

Based on the Arnold transform, the elements of the sparse matrix $\boldsymbol{SM}$ are scrambled, and the disordered sparse matrix $\boldsymbol{SSM}$ is obtained, first scrambling the image, which is conducive to reducing the blocking effect in image compression[17]. With the decrease of bit rate, quantization becomes rough and discontinuity appears at the boundary of block, which affects the reconstructed image.

In order to compress the image, the key stream Q_1 generated by QCNN hyperchaotic system is used to construct the measurement matrix. From Q_1, the method of step size 2 is adopted, that is, sampling once every interval of an element. The length of the sampling element is M×N, and the sampling result is recorded as QS:

$$QS=Q_1(2\times j), \quad (4)$$

where j=1,2,…, M×N.

The sampling results are normalized and mapped to positive real numbers between (0,1):

$$NQS=\mathrm{mod}(QS\times 10^{14}, 1), \quad (5)$$

where mod () is the modular function.

Then, the normalized sampling results are transformed into M×N measurement matrix $\boldsymbol{\phi}$ according to the order from top to bottom and from left to right:

$$\boldsymbol{\phi}=\mathrm{reshape}(NQS, M, N), \quad (6)$$

where reshape() is the matrix deformation function, M is the number of rows of the measurement matrix, and the

compression ratio is $CR=M/N$.

According to the theory of compressed sensing, the measurement matrix $\boldsymbol{MVM}$ is obtained by sampling the disordered sparse matrix $\boldsymbol{SSM}$ with measurement matrix $\boldsymbol{\phi}$. Each element value of the measurement matrix $\boldsymbol{MVM}$ is mapped to an integer between 0 and 255, and the integer mapping of $\boldsymbol{MVM}'$ is obtained, which is converted into a one-dimensional sequence with length of $M\times N$:

$$\begin{cases} \boldsymbol{MVM} = \boldsymbol{\phi} \times \boldsymbol{SSM} \\ \boldsymbol{MVM}^{'} = \text{reshape}(\text{floor}(\dfrac{255\times(\boldsymbol{MVM}-\min)}{\max-\min}),1,M\times N) \end{cases}, \quad (7)$$

where floor () is the downward rounding function, where max and min represent the maximum and minimum element values in the measurement matrix $\boldsymbol{MVM}$, respectively.

The key stream Q_2 generated by the QCNN hyperchaotic system is sorted from small to large, and the index matrix $\boldsymbol{PQ}_2$ is obtained. The measured value matrix $\boldsymbol{MVM}'$ is scrambled by the index matrix $\boldsymbol{PQ}_2$, and the disordered measurement value matrix $\boldsymbol{SMVM}$ is obtained.

$$\begin{cases} [\sim, \boldsymbol{PQ}_2] = \text{sort}(Q_2) \\ \boldsymbol{SMVM} = \boldsymbol{MVM}^{'}(\boldsymbol{PQ}_2) \end{cases}. \quad (8)$$

In order to perform bidirectional diffusion operation on the disordered measurement matrix $\boldsymbol{SMVM}$, the key streams Q_3 and Q_4 generated by QCNN hyperchaotic system are mapped to integers between 0 and 255:

$$\begin{cases} \boldsymbol{NQ}_3 = \text{mod}(\text{floor}(Q_3\times 10^{14}),256) \\ \boldsymbol{NQ}_4 = \text{mod}(\text{floor}(Q_3\times 10^{14}),256) \end{cases}. \quad (9)$$

Using $\boldsymbol{NQ}_3$ to forward diffuse the disordered measurement matrix $\boldsymbol{SMVM}$, the forward diffusion measurement matrix $\boldsymbol{FSMVM}$ is obtained.

$$\begin{cases} \boldsymbol{FSMVM}(1) = \boldsymbol{SMVM}(1) \oplus \boldsymbol{NQ}_3(1) \\ \boldsymbol{FSMVM}(i) = \boldsymbol{SMVM}(i) \oplus \boldsymbol{NQ}_3 \oplus \boldsymbol{FSMVM}(i-1) \end{cases}, \quad (10)$$

where i=2,3,…, $M\times N$, and $\oplus$ is XOR operation.

The matrix $\boldsymbol{FSMVM}$ is backward diffused by $\boldsymbol{NQ}_4$, and the backward diffusion measurement matrix $\boldsymbol{BSMVM}$ is obtained.

$$\begin{cases} \boldsymbol{BSMVM}(M\times N) = \boldsymbol{FSMVM}(M\times N) \\ \qquad\qquad \oplus \boldsymbol{NQ}_4(M\times N) \\ \boldsymbol{BSMVM}(i) = \text{mod}((\boldsymbol{FSMVM}(i) \\ \qquad + \boldsymbol{BSMVM}(i+1)),256) \oplus \boldsymbol{NQ}_4(i) \end{cases}, \quad (11)$$

where $i= M\times N-1,\ldots,2,1$.

Finally, the matrix $\boldsymbol{BSMVM}$ is transformed into a matrix with the size of $M\times N$, that is, the encrypted ciphertext image is obtained.

The decryption process is the reverse process of encryption process, and the specific process is shown in Fig.6. The symmetric security key generated by QNCC hyperchaotic system is applied to reverse scrambling and reverse scrambling operation respectively. At the same time, the OMP[18] algorithm is used for image reconstruction. Using the position scrambling order generated by Arnold chaotic system, the image is scrambled inversely. Finally, the final decryption image is obtained by inverse discrete wavelet transform.

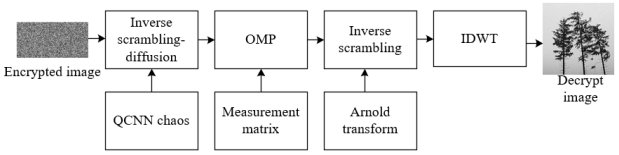

Fig.6 Decryption process block diagram

Verify the effect and performance of the scheme, the numerical simulation is based on MATLAB 2015b software, and the simulation operating system is windows 10. The simulation computer is configured with Inter©Core™i5-9300H CPU@2.40 GHz memory of 8 GB. We do the following simulation experimental analysis on two range-gated laser images "tree" and "wall" with the size of 256×256 pixels.

When CR is 0.5, the encryption and decryption results of distance gated laser images "tree" and "wall" are shown in Fig.7. As shown in Fig.7(b) and Fig.7(e), the size of the encrypted image after secure compression is half of the original image. For the decrypted image, Fig.7(c) and Fig.7(f) restore the shape of the original image from the perspective of subjective visual effect. The simulation results show that the scheme successfully compresses and encrypts the original image, and according to the characteristics of laser imaging, the decrypted and reconstructed image has no visual loss.

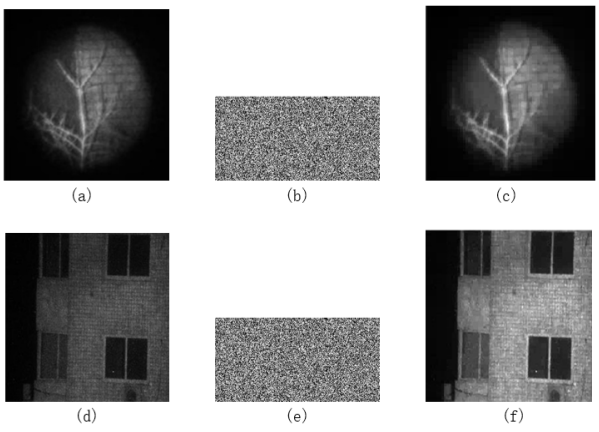

Fig.7 Image encryption and decryption result

In order to further quantitatively evaluate the secure compression encryption scheme of range-gated laser imaging, the peak signal-to-noise ratio ($PSNR$) is used to compare the quality of processed images. The definition is as follows[19]:

$$PSNR = 10\times\lg\frac{255\times 255}{\frac{1}{N^2}\times\sum_{i=1}^{N}\sum_{j=1}^{N}(I(i,j)-I^{'}(i,j))^2}, \quad (12)$$

where I and I' represent the pixel values of the original image and the decoded image respectively, and $N\times N$ represents the size of the image. The higher the *PSNR* value, the higher the similarity between the original image and the decrypted image. Tab.1 lists the *PSNR* of the original and decrypted images at compression ratios of 0.25, 0.5 and 0.75, respectively. It can be seen from the table that the *PSNR* values of the above three compression ratios are all around 30 dB, the results show that the proposed method has good compression reconstruction performance.

Tab.1 *PSNR* values of different compression ratios

Original image	*CR*	*PSNR* (dB)
"tree"	0.25	35.407 0
	0.5	36.354 6
	0.75	36.503 6
"wall"	0.25	29.651 5
	0.5	34.057 2
	0.75	34.194 6

Histogram is a function image which counts the number of points with the same pixel value, it can directly display the distribution of image pixel value. Usually, the pixel value distribution of the original image will be uneven. In order to ensure the security of information, the histogram of the encoded image should be as flat as possible[20]. Fig.8 shows the histogram of the pixel value distribution of the original image and the encrypted image. It can be seen that the pixel value distribution of the encrypted image is very uniform. Without losing generality, this paper analyzes the difference between the histogram of the original image and the encrypted image in Fig.8, and uses the standard deviation as the quantization standard. For sample space $\{X_i\}$, i=0,1,…,255, the standard deviation of the sample is calculated as follows[21]:

$$s=\sqrt{\frac{1}{256}\sum_{i=0}^{255}(X_i-E(X))^2}\ . \tag{13}$$

For a 256×256 image, $E(X)$=256, X_i represents the frequency of pixels with a value of i, and s is the sample standard deviation of histogram. Tab.2 lists the sample standard deviation of original image and encrypted image histogram. It can be seen from the table that the sample standard deviation of the image histogram is about 10, which is much smaller than the sample standard deviation of the original image. It is proved that the histogram of encrypted image is smoother than that of original image. Therefore, this method can well hide the distribution information of image pixel value, and has good anti-statistical analysis ability.

Information entropy is an important index to evaluate the randomness of an image. It is essentially the average number of each pixel in the image. When the image is 256 gray level, the ideal information entropy is 8. Tab.3 lists the information entropy of the original images and encrypted images in Fig.8. It can be seen from the table that the information entropy of the encrypted image is close to the ideal information entropy. The results show that the encrypted image generated by our scheme has good statistical characteristics similar to random image, and can resist statistical attacks well.

Tab.2 Sample standard deviation of histogram

Image	*CR*	"tree"	"wall"
Original image		900.06	431.51
Encrypted image	0.25	7.48	7.59
	0.5	10.54	10.67
	0.75	14.45	12.84

Tab.3 Information entropy

Image	*CR*	"tree"	"wall"
Original image		5.883 0	6.393 6
Encrypted image	0.25	7.990 2	7.989 8
	0.5	7.995 1	7.995 0
	0.75	7.995 9	7.996 7

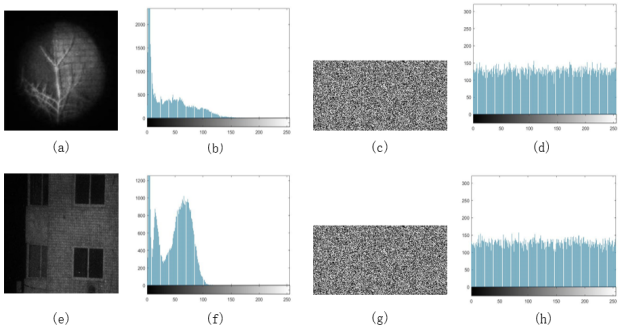

Fig.8 Histogram results: (a) (e) Original images; (b) (f) Original image histograms; (c) (g) Encrypted images; (d) (h) Encrypted image histograms

Image transmission is affected by various noises. In order to decrypt the image correctly, a good image encryption algorithm should have the ability to resist the noise attack. Salt and pepper noise (SPN) and Gaussian noise (GN) are two common noises. Different intensities of noise are added to the encrypted image of "tree". Fig.9 shows that salt and pepper noise with intensity of 1×10^{-5} and 5×10^{-5}, and Gaussian noise with mean value of 0, intensity of 2×10^{-7} and 3×10^{-7} are added to the encrypted image of "tree". It can be seen that in the case of low resolution and poor definition, the decrypted image can display the information of the original image. Therefore, this method has better ability to resist noise attack.

A secure compression encryption scheme for gated-laser imaging based on compressive sensing and bidirectional diffusion is proposed. Based on the analysis of the characteristics of laser ranging image acquisition, the discrete wavelet transform is used to sparse the laser image, and the chaotic system is used to confuse the im-

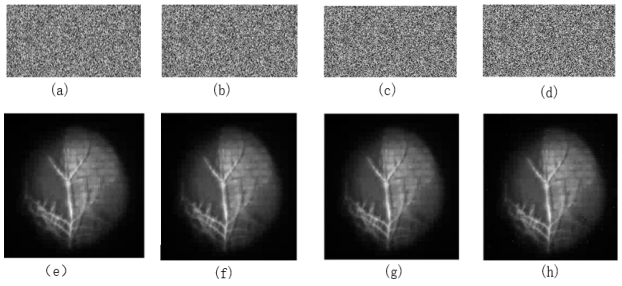

Fig.9 The experimental results of adding noise: (a) (e) Encrypted and decrypted images with salt and pepper noise intensity of 1×10^{-5}; (b) (f) Encrypted and decrypted images with salt and pepper noise intensity of 5×10^{-5}; (c) (g) Encrypted and decrypted images with Gaussian noise intensity of 2×10^{-7}; (d) (h) Encrypted and decrypted images with Gaussian noise intensity of 3×10^{-7}

age pixels. Combined with QCNN hyperchaotic system, the image is measured, quantized, compressed, and bidirectional diffused. The secure compression and encryption of gated laser image is realized, and the image reconstruction is completed through encryption reverse operation at the receiving end. Experimental results show that the compression encryption method has good security and can resist various statistical analysis and noise attacks. At the same time, the encryption method effectively reduces the amount of data transmitted in the channel and improves the transmission efficiency. The results show that the secure compression encryption method combining compressed sensing and QCNN are feasible and applicable in gated laser image compression and encryption.

References

[1] Wang Shu-yu, Tao Sheng-xiang, Chen Dong and Gu Guo-hua, Optoelectronics Letters **15**, 21 (2019).

[2] Andresen Bjørn F, Steinvall Ove, Fulop Gabor F, Andersson Pierre, Elmqvist Magnus, Norton Paul R and Tulldahl Michael, Proceedings of SPIE **6542**, 654216 (2007).

[3] Huckridge David A, Göhler B, Ebert Reinhard R, Lutzmann P and Anstett G, Proceedings of SPIE **7113**, 711307 (2008).

[4] Kamerman Gary W, Laurenzis Martin, Steinvall Ove, Christnacher Frank, Bacher Emmanuel, Bishop Gary J, Gonglewski John D, Metzger Nicolas, Schertzer Stéphane, Lewis Keith L, Hollins Richard C, Scholz Thomas and Merlet Thomas J, Proceedings of SPIE **8186**, 818603 (2011).

[5] Merritt Paul and Kramer Mark, Proceedings of SPIE **3086**, 2 (1997).

[6] Guan Bin and He Da-hua, Optics & Optoelectronic Technology **15**, 10 (2017). (in Chinese)

[7] Lv Wen-lei, Xu Zhang and Ke Liu, Journal of Ordnance Equipment Engineering **40**, 199 (2019). (in Chinese)

[8] Chen Xiaodong, Di Xiaoqiang, Li Jinqing, Zhao Jianping, Liu Xiaojie, Yu Hui, Pu Yifei, Li Chunming and Pan Zhigeng, Proceedings of SPIE **11069**, 174 (2019).

[9] Man Zhenlong, Li Jinqing, Di Xiaoqiang and Bai Ou, IEEE Access **7**, 103047 (2019).

[10] Yuan Han-qin, Journal of CAEIT **14**, 831 (2019). (in Chinese)

[11] Daniel Herrera C, Juho Kannala and Janne Heikkila, IEEE Trans. Pattern Anal. Mach. Intell. **34**, 2058 (2012).

[12] Xie Meilin, Liu Peng, Ma Caiwen, Huang Wei, Liang Jian and Feng Xubin, Optik **157**, 556 (2018).

[13] Donoho D. L, IEEE Transactions on Information Theory **52**, 1289 (2006).

[14] CANDÈS EMMANUEL J., ROMBERG JUSTIN K. and TAO TERENCE, Communications on Pure and Applied Mathematics **59**, 1207 (2006).

[15] FORTUNA LUIGI and PORTO DOMENICO, International Journal of Bifurcation and Chaos **14**, 1085 (2004).

[16] Wu Chuhan, Chang Jun, Quan Chenggen, Zhang Xiaofang and Zhang Yongjian, Results in Optics **1**, 100021 (2020).

[17] Wu Ming Te, Information Sciences **474**, 125 (2019).

[18] Tropp Joel A and Gilbert Anna C, IEEE Transactions on Information Theory **53**, 4655 (2007).

[19] Chai Xiuli, Gan Zhihua, Yang Kang, Chen Yiran and Liu Xianxing, Signal Processing: Image Communication **52**, 6 (2017).

[20] Pak Chanil and Huang Lilian, Signal Processing **138**, 129 (2017).

[21] Zhang Yong, Chen Aiguo, Tang Yingjun, Dang Jianwu and Wang Guoping, Information Sciences **526**, 180 (2020).