A Remote Security Computational Ghost Imaging Method Based on Quantum Key Distribution Technology

JIANAN WU\textsuperscript{1,2}, YUN CHEN\textsuperscript{2}, CHENG ZHOU\textsuperscript{3,4}, ZHONGYANG CHEN\textsuperscript{2}, CHENGQIAN XU\textsuperscript{1}, AND LIJUN SONG\textsuperscript{4,5}

\textsuperscript{1}College of Computer Science and Technology, Changchun University, Changchun 130022, China
\textsuperscript{2}College of Network Security, Changchun University, Changchun 130022, China
\textsuperscript{3}Center for Quantum Sciences and School of Physics, Northeast Normal University, Changchun 130024, China
\textsuperscript{4}Jilin Engineering Laboratory for Quantum Information Technology, Changchun 130052, China
\textsuperscript{5}Jilin Vocational College of Industry and Technology, Jilin 132013, China

Corresponding author: Lijun Song (ccdxslj@126.com)

This work was supported in part by the Innovation Capacity Building Project of the Jilin Provincial Development and Reform Commission under Grant 2020C020-2, and in part by the Innovation Platform and Talent Project of Jilin Provincial Department of Science and Technology under Grant 20210506043ZP.

\textbf{ABSTRACT} Computational ghost imaging (CGI) is a method of acquiring object information by measuring light field intensity, which would be used to achieve imaging in a complicated environment. The main issue to be addressed in CGI technology is how to achieve rapid and high-quality imaging while ensuring the secure transmission of detection data in practical distant imaging applications. In order to address the mentioned issues, this paper proposes a remote secure CGI method based on quantum communication technology. Using the quantum key distribution (QKD) network, the CGI system can be reconstructed while solving the problem of information security transmission between the detector and the reconstructed computing device. By exploring the influence of different random measurement matrices on the quality of image reconstruction, it is found that the randomness of the numerical sequence constituting the matrix is positively correlated with the imaging quality. Based on this discovery, a new type of quantum cryptography measurement matrix is constructed using quantum cryptography with good randomness. In addition, through further orthogonalization and normalization of the matrix, the matrix has both good randomness and orthogonality, and high-quality imaging results can be obtained at a low sampling rate. The feasibility and effectiveness of the method are verified by simulation imaging experiments. Compared with the traditional GI system, the method proposed in this paper has higher transmission security and high-quality imaging under this premise, which provides a new idea for the practical development of CGI technology.

\textbf{INDEX TERMS} Computational ghost imaging, quantum key distribution, quantum cryptography, measurement matrix, randomness, schimidt orthogonalization.

\textbf{I. INTRODUCTION} In recent years, the performance of core array sensors such as charge-coupled device (CCD) cameras or complementary metal-oxide-semiconductor (CMOS) cameras can no longer meet the imaging requirements in complex environments, such as low light imaging, non-line-of-sight imaging, and imaging through scattering media. Seeking a new imaging solution from both the perspective of imaging equipment and a new imaging method is an effective way to solve this problem. Correlation imaging, also known as ghost imaging (GI) [1], is an effective imaging scheme. Unlike traditional methods, it achieves the separation of detection and imaging, thus allowing the reconstruction of objects in more complex environments. GI has been applied many fields, including gas imaging [2], infrared imaging [3], underwater imaging [4]–[6], microscopic imaging [7], three dimensional imaging [8]–[10], scattering medium imaging [11], and x-ray imaging [12].

GI is created by correlating the total light signal reflected from the target collected by the bucket detector with the reference spatial light distribution signal collected by the
multi-pixel array detector. In 2008, Shapiro and Jeffrey [13] proposed a CGI system that requires only one bucket detector and spatial light modulation equipment. Later, Bromberg et al. [14] performed an experimental demonstration. CGI is a useful imaging technique that can be accomplished only using a bucket detector with no spatial resolution. The specific process is that the bucket detector measures the total intensity of the overlap between the object and a set of patterns, and then the measurements are combined with the mask knowledge to reconstruct the image. With the progress of CGI, spatial light modulator (SLM) [13], [14] or digital micro-mirror device (DMD) have started to be used to generate random patterns. The measurement matrix is a matrix that is formed by several random patterns through certain transformations. The construction of the measurement matrix determines the patterns and thus affects the quality of the CGI imaging.

Orthogonal matrices, including the Fourier-derived matrix [11], the Hadamard-derived matrix [15]–[19], etc., have short reconstruction times and good reconstruction performance, but reduced interdependence between column vectors. In addition, the Fourier matrix is only independent of the time domain signals while the dimension of the Hadamard-derived matrix must be $2^N$, which limits its application in practice. Random measurement matrices mainly include Bernoulli random matrices [20], random sparse measurement matrices, Gaussian random measurement matrices [21], sub-Gaussian random matrices [22], etc. They have the advantage that they are incoherent with most sparse signals, and the number of measurements required for accurate reconstruction is small. In practical application scenarios, the random measurement matrix has an advantage over the orthogonal matrix. However, with less detection, the noise is high, and it is harder to image clearly. Constructing measurement matrices with both randomness and orthogonality to improve the efficiency of CGI is a problem to be solved. CGI systems is usually composed of a light source, an optical field modulation device, a lens, a target object, and a detector. The light source is irradiated on the object to be measured through the light field modulation device and collected as a data signal (called detection data) by a detector [23]. CGI technology faces some problems in the fields of deep-sea monitoring, remote sensing imaging, military detection, and other long-distance imaging. It is a difficult challenge to ensure the safe and fast transmission of detected data to the remote computing nodes.

Quantum key distribution (QKD) technology [24] is a method of securing information by physical means. Its security comes from two properties of quantum mechanics. Firstly, the quantum world is truly random, which is the key to generating truly random keys and the main factor that can produce highly random quantum cryptography sequences. Second, a single quantum state carrying non-orthogonal information cannot be perfectly replicated [25], [26]. Due to the unconditional security of the QKD system [27], [28], it provides help to solve the critical data transmission problem by remote computational ghost imaging. Meanwhile, the quantum cryptography generated by the QKD system has good randomness and can be used as a data source for constructing measurement matrix.

In chapter 2, this paper describes the shortcomings of current CGI techniques and mentions the relevant theoretical foundations required in this work, including the QKD technique based on the BB84 protocol and the random number randomness testing principles and methods. Chapter 3 describes details of the remote, secure CGI scheme based on the QKD technique, complete with a description of the quantum cryptography measurement matrix construction and optimization. Numerical simulations are used in chapter 4 to verify the feasibility of the CGI system scheme proposed in this thesis and to demonstrate the advantages of the newly constructed measurement matrix for imaging. Finally, we give the conclusion of this paper in the last chapter.

The contribution of this paper consists of two main points. Firstly, we designed a remote, secure CGI scheme based on QKD technology, which improves the CGI system and promotes its practicality. Secondly, a quantum cryptography measurement matrix with both randomness and orthogonality is constructed to improve the efficiency of the imaging while innovating a new CGI system.

II. CORRELATION THEORY
A. COMPUTATIONAL GHOST IMAGING PRINCIPLES

Traditional ghost imaging (pseudo-thermal ghost imaging) works on the following principle. The coherent light field generated by the laser is changed into randomly scattered light fields by the rotating ground glass and divided into two beams by the beam splitter. One of the beams is focused by a convex lens after passing through the object, and its total intensity is measured by a bucket detector without resolution. The other beam is free to propagate for a certain distance, and then the light field distribution is detected by a CCD camera. The light intensity (detection data) measured by the two detectors is correlated to obtain the image of the object to be measured. The experimental setup is shown in Fig. 1.

![FIGURE 1. Traditional GI system diagram.](image-url)
omitting the reference optical path, the signal optical path is the same as that of the traditional pseudo-thermal GI system, and single optical path imaging is achieved. The experimental setup is shown in Fig. 2.

The intensity of the light field reflected by the target object is collected by a bucket detector. Image reconstruction is performed in computer using the correlation algorithm [29]–[31]. When improving imaging systems, CGI researchers have found that the spatial light field (Area B in Fig. 2), which has been preset by SLM or DMD, has a large impact on the imaging efficiency, so attention is put on the spatial light field (measurement matrix) design.

The measurement matrices commonly used today are divided into those with randomness and orthogonality (Hadamard) as shown in Fig. 3. The use of quantum cryptography with high randomness to construct a new measurement matrix to form a mask (Area B in Fig. 2) can improve the efficiency of imaging.

B. QKD PRINCIPLE
The existing actual QKD system mainly adopts BB84 protocol [26], and the principle is shown in Fig. 4. Alice randomly selects one of the four BB84 states to prepare a single-photon quantum state, which is then sent to Bob via a quantum channel. After Bob receives the quantum state from Alice, he randomly selects one of the Z and X basis vectors for measurement and records the result. Alice and Bob then compare the encoded and measured basis vectors through the public authentication channel, keeping the encoded bits and measurements of the same basis vector, thus obtaining a string of original keys. Assuming the ideal situation of no eavesdropper Eve attack, no interference in the channel, and no dark count in the detector, the original key string of Alice and Bob will be exactly the same. In practice, there is some error in the original key of Alice and Bob due to the channel noise, the dark count of the detector, and the possible eavesdropping of Eve.

Alice and Bob can obtain an estimate of the BER by sampling a random public fraction of bits. If the BER exceeds a certain theoretical threshold, the original key string is discarded and the process is repeated. Otherwise, a secure key string is obtained through post-processing of the data, such as error correction and privacy amplification. Alice and Bob at both ends of the communication obtain the same quantum key.

C. RANDOM NUMBER
Random number plays a very important role in QKD systems. Random numbers include truly random numbers (TRN) and pseudo-random numbers (PRN). Pseudo-random numbers are generated by the pseudo-random number generator (PRNG) using a deterministic algorithm and a short sequence of random seeds to generate a long sequence of random numbers. Ideal random numbers are also known as true random numbers, and physical random number is a random sequence obtained by observing uncertain physical processes, which are by far the closest random sequences to true randomness. Physical random number generators are divided into two types, classical noise-based random number generators and quantum noise-based random number generators. The former uses noise sources that can be described by classical physics, such as thermal noise of electronic components and chaotic random number generators. This type of random number generator is pseudo-random in terms of specific physical principles and thus has some hidden dangers in practice. The quantum random number generator (QRNG) is the only random number generator so far that is theoretically capable of generating completely unpredictable random sequences based on quantum intrinsic randomness.

The basic theory of randomness testing [32] is the basic technique of hypothesis testing. The NIST test suite, which has 15 test items [33], [34], is used in this thesis to test the randomness of binary sequences. Each test is based on a hypothesis test, uses a different test principle to represent a different aspect of the random test.

D. IMAGE QUALITY EVALUATION METHOD
Peak signal-to-noise ratio (PSNR) [35] is a widely used method to evaluate the quality of reconstructed imaging, which is closely related to mean square error. Mean square error (MSE) in ghost imaging refers to the expectation of the square of the difference between the reconstructed image value and the real image value. It is a convenient method to measure the “average error” of the reconstructed image. MSE is an objective measure of the deviation between the pixel value and the true value of all pixels in the image. They are defined as follows:

$$MSE = \frac{1}{a \times b} \sum_{x,y=1}^{a,b} [T(x, y) - G(x, y)]^2, \quad (1)$$
where $T(x, y)$ is the original image pixel point value, $G(x, y)$ is the reconstructed image pixel point value.

\[
PSNR = 10 \log \left( \frac{(2^n - 1)^2}{MSE} \right),
\]

where, $n$ is the number of bits per pixels.

Therefore, the larger the PSNR value, the clearer the reconstructed image, and the smaller the PSNR value, the more blurred the reconstructed image.

III. SYSTEM PRINCIPLE AND DESIGN

A. REMOTE SECURITY GHOST IMAGING SYSTEM BASED ON QKD

1) SYSTEM SCHEME DESIGN

In this paper, a QKD network-based CGI system for remote secure communication is designed, and the architecture is shown in Fig. 5. This system contains three main parts. Module A is a point-to-point quantum confidentiality communication unit, which mainly contains two communication nodes, Alice and Bob. Based on QKD technology, both parties can generate a symmetric quantum cryptography sequence (QCS), which can be used as the data source for constructing the quantum cryptography measurement matrix and the key for message transmission between Module B and Module C. Module B is the detection unit, which mainly includes the measurement matrix generation component based on the quantum cryptography random sequence and the computational ghost imaging component. The measurement matrix component is mainly used to generate the quantum cryptography measurement matrix (QCM) and quantum cryptography pattern (QCP). The computational ghost imaging component consists of optical devices such as laser light source, SLM, detector, and lens, which are used to collect key data for imaging the target object. Module C is the reconstruction unit, which mainly includes the measurement matrix generation component and the image reconstruction component to realize the target object reconstruction.

Fig. 6 shows the actual structure of the system. Combined with Fig. 5, the system imaging process is as follows:

Step 1: Alice and Bob in the QKD component simultaneously generate equivalent QCS through QKD technology.

Step 2: The measurement matrix generation component downloads enough QCS converts it into QCP and sends it to the computational ghost imaging component for detecting the target image.

Step 3: In the ghost imaging component, the light source is projected onto the target object after SLM modulation, and the detection value collected by the bucket detector are sent to Bob.

Step 4: The quantum key used by the encryption engine in Bob encrypts the detection value in a one-time encryption mode.
Step 5: The encrypted detection value is transmitted to Alice using the classic channel between Alice and Bob in the QKD system.

Step 6: The decryption engine in Alice decrypt the detection value of the cipher-text into plain-text using the same quantum key as in step 4.

Step 7: Alice sends the plain-text detection value to the image reconstruction component.

Step 8: The measurement matrix generation component in module C downloads the same QCS as in step 2 and converts it into QCM.

Step 9: The measurement matrix generation component sends the QCM to the image reconstruction component to calculate the target object.

2) SYSTEM SECURITY ANALYSIS

As shown in Fig. 7, the system contains potential security issues at point ①, ② and ③. This section provides a detailed analysis of the security of the above three points.

The whole system connects LANs A and B with quantum communication technology. The point ② common channel is composed of quantum communication technology to transmit the data packets from LAN B to LAN A. Usually, Alice and Bob use the quantum channel and the classical channel to obtain the equivalent amount of quantum cryptography, where quantum cryptography plays two main roles. The first role is to encrypt the data as a key. The second role is as the source of data for the measurement matrix of CGI. Therefore, the distribution of quantum cryptography is crucial in this system. The quantum key distribution at point ② has unconditional security in theory.

The point ④ (Alice to module C) and the point ⑤ (Bob to module B) belong to the same LAN and are set as confidence intervals.

B. QUANTUM CRYPTOGRAPHY MEASUREMENT MATRIX DESIGN

1) MATRIX CONSTRUCTION

The steps of converting QCS to QCM are as follows:

Step 1: Take a QCS of length \( m \times m \) and convert it into a matrix of \( m \times m \) in the original order. Where \( m \) is the number of rows and columns of the target object. \( I_i(x, y) \) represents the spatial intensity distribution of the \( i \)th QCP.

\[
I_i(x, y) = QCS_i = \begin{bmatrix} I_{i1} & I_{i2} & \cdots & I_{im}^{(m-1)} & I_{im}^{m \times m} \end{bmatrix},
\]

(3)

Step 2: Use MATLAB image processing function to convert \( I_i(x, y) \) into QCP. If clear imaging need to detect the target object \( n \) times, then need to repeat Step 1 for \( n \) times.

Step 3: QCM consists of \( n \) rows of QCP in total. The formation process of QCM is shown in
The formation process of quantum cryptography measurement matrix.

**FIGURE 8.** The formation process of quantum cryptography measurement matrix.

The matrix of bucket detection values can be expressed as

$$B_i = \begin{bmatrix} I_1^1 & I_2^1 & \cdots & I_i^1 & \cdots & I_n^1 \\ I_1^2 & I_2^2 & \cdots & I_i^2 & \cdots & I_n^2 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ I_1^m & I_2^m & \cdots & I_i^m & \cdots & I_n^m \end{bmatrix} \times \begin{bmatrix} O_1 \\ O_2 \\ \vdots \\ O_{n-1} \\ O_n \end{bmatrix},$$

(7)

**C. SCHMIDT ORTHOGONALIZATION**

The Schmidt orthogonalization [36] is a method that enables the orthogonality of matrices, and we use this method to add new properties to the QCM, which is shown in Fig. 9(a). The procedure is as follows:

Step 1: Eq. (3) is brought into Eq. (5) to obtain Eq.(8).

**FIGURE 9.** Schematic diagram of quantum cryptography measurement matrix.

Fig. 8 (Let n be equal to 4).

$$QCM = \begin{bmatrix} I_1(x, y) \\ I_2(x, y) \\ \vdots \\ I_i(x, y) \\ \vdots \\ I_{n-1}(x, y) \\ I_n(x, y) \end{bmatrix},$$

(4)

The transpose matrix of Eq.(2) is as Eq.(5), shown at the bottom of the page.

The bucket detector measurements result were $B_i$ [19].

$$B_i = \iint I_i(x, y)O_i(x, y)dx\,dy, \quad (6)$$

where $O_i(x, y)$ is the value of the target $(x, y)$ point of the $i$th detection.

$$QCM = \begin{bmatrix} I_1^1 & I_2^1 & \cdots & I_i^1 & \cdots & I_n^1 \\ I_1^2 & I_2^2 & \cdots & I_i^2 & \cdots & I_n^2 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ I_1^m & I_2^m & \cdots & I_i^m & \cdots & I_n^m \end{bmatrix}$$

(8)

Step 2: Using $\gamma$ to represent the column vector, Eq. (9) can be expressed as

$$QCM = \begin{bmatrix} I_1^1 & I_2^1 & \cdots & I_i^1 & \cdots & I_n^1 \\ I_1^2 & I_2^2 & \cdots & I_i^2 & \cdots & I_n^2 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ I_1^m & I_2^m & \cdots & I_i^m & \cdots & I_n^m \end{bmatrix}$$

$$= \begin{bmatrix} I_1 & I_2 & \cdots & I_i & \cdots & I_n \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ I_{n-1} & I_{n-1} & \cdots & I_{n-1} & \cdots & I_{n-1} \\ I_n & I_n & \cdots & I_n & \cdots & I_n \end{bmatrix}$$

(9)

$$QCM^T = \begin{bmatrix} I_1(x, y) & I_2(x, y) & \cdots & I_i(x, y) & \cdots & I_{n-1}(x, y) & I_n(x, y) \end{bmatrix},$$

(5)
TABLE 1. NIST test results.

| N | Test Item | Sequence-A | Sequence-B | Sequence-C |
|---|-----------|------------|------------|------------|
| 1 | Frequency | .. | 0.162606 | 0.837119 |
| 2 | Block Frequency | .. | 0.911413 | 0.275709 |
| 3 | Cumulative Sums(Forward) | .. | 0.275709 | 0.739918 |
| 4 | Cumulative Sums(Reverse) | .. | 0.739918 | 0.834308 |
| 5 | Runs | .. | 0.275709 | 0.035174 |
| 6 | Longest Run | .. | 0.275709 | 0.739918 |
| 7 | Rank | 0.06199 | 0.213309 | 0.250485 |
| 8 | DFT | 0.911413 | 0.437274 | 0.739918 |
| 9 | Non-Overlapping Template | 0.122325 | 0.991468 | 0.999438 |
| 10 | Overlapping Template | 0.002043 | 0.637119 | 0.666882 |
| 11 | Universal | .. | 0.350485 | 0.162606 |
| 12 | Approximate Entropy | .. | 0.213309 | 0.964295 |
| 13 | Random Excursions | .. | 0.090936 | 0.060936 |
| 14 | Random Excursions Variant | .. | 0.090936 | 0.025193 |
| 15 | Serial(1) | 0.350485 | 0.834308 | 0.437274 |
| 16 | Serial(2) | 0.739918 | 0.964295 | 0.275709 |
| 17 | Linear Complexity | 0.122325 | 0.637119 | 0.637119 |

Step 3: Bring Eq. (8) into Eq. (9) to obtain Eq. (10).

\[
QCM = \begin{bmatrix}
I_1(x, y) \\
I_2(x, y) \\
\vdots \\
I_i(x, y) \\
\vdots \\
I_n-1(x, y) \\
I_n(x, y)
\end{bmatrix}
= \begin{bmatrix}
\gamma_1 \\
\gamma_2 \\
\vdots \\
\gamma_i \\
\vdots \\
\gamma_{n-1} \\
\gamma_n
\end{bmatrix}, \quad (10)
\]

Step 4: For each column vector in Eq. (10), perform the transformation of Eq. (11) so that each column vector is orthogonal to each other to obtain the orthogonal matrix, as shown in Eq. (13).

\[
\hat{\gamma}_1 = \gamma_1, \\
\hat{\gamma}_2 = \gamma_2 - c_{21} \hat{\gamma}_1, \\
\hat{\gamma}_3 = \gamma_3 - c_{32} \hat{\gamma}_2 - c_{31} \hat{\gamma}_1, \\
\vdots \\
\hat{\gamma}_{m \times m} = \gamma_{m \times m} - c_{m \times (m-1)} \hat{\gamma}_1,
\]

where

\[
c_{ij} = \frac{\langle \hat{\gamma}_i \cdot \gamma_j \rangle}{\| \gamma_j \|_2^2}, \quad (12)
\]

\[
SO - QCM = \begin{bmatrix}
\hat{\gamma}_1 \\
\hat{\gamma}_2 \\
\vdots \\
\hat{\gamma}_i \\
\vdots \\
\hat{\gamma}_{n-1} \\
\hat{\gamma}_n
\end{bmatrix}, \quad (13)
\]

Step 6: From Eq. (13) and Eq. (14) can obtain the quantum cryptography matrix after final orthogonal normalization (SON-QCM) and the corresponding pattern is shown in Fig. 9(c). The quantum cryptography pattern with both random and orthogonal properties is converted from a quantum cryptography measurement matrix after orthogonal normalization.

\[
SQN - QCM = \begin{bmatrix}
\vartheta_1 \\
\vartheta_2 \\
\vdots \\
\vartheta_i \\
\vdots \\
\vartheta_{n-1} \\
\vartheta_n
\end{bmatrix}
= \begin{bmatrix}
v_1(x, y) \\
v_2(x, y) \\
\vdots \\
v_i(x, y) \\
\vdots \\
v_{n-1}(x, y) \\
v_n(x, y)
\end{bmatrix}, \quad (15)
\]

IV. NUMERICAL SIMULATION RESULTS

A. IMAGING PERFORMANCE ANALYSIS OF THE QUANTUM CRYPTOGRAPHY MATRIX

1) RANDOMNESS TEST OF MATRIX NUMERICAL SEQUENCE

In order to verify the influence of randomness of number sequence of measurement matrix on imaging results, three numerical sequences Sequence-A, Sequence-B and Sequence-C from different sources were used as data sources of measurement matrix. Sequence-A failed the NIST test and was a non-random sequence. Sequence-B is a pseudo-random sequence generated by Matlab built-in functions. Sequence-C is a true random sequence composed of quantum codes generated by QKD system. US statistical test suite published by the NIST (V2.1.2) is used to verify the randomness of Sequence-A, Sequence-B and Sequence-C. As can be seen from the test results (p-values) of NIST shown in Tab. 1, sequence-C shows good randomness.

2) IMAGING QUALITY ANALYSIS

We take the logo ‘gong’ of Industrial and Commercial Bank of China as the target object with the size of 32 × 32 pixels.
J. Wu et al.: Remote Security Computational Ghost Imaging Method Based on Quantum Key Distribution Technology

FIGURE 10. (a) Sequence-A measurement matrix reconstruction image results, (b) Sequence-B measurement matrix reconstruction image results, (c) Sequence-C measurement matrix reconstruction image results.

FIGURE 11. (a) SO-QCM reconstruction image results, (b) QCM reconstruction image results.

(see Fig. 10 Object), and use the Sequence-A, Sequence-B and Sequence-C measurement matrix to carry out numerical simulation of CGI. The second-order correlation imaging results show that the Sequence-A measurement matrix can’t reconstruct the image information, while the Sequence-B and Sequence-C measurement matrix can successfully obtain the image information, and the image quality gradually increases with the increase of measurement times. Moreover, it can be seen from the calculated PSNR that the reconstructed image quality obtained by using the Sequence-C measurement matrix generated by quantum cryptography is higher than that of the Sequence-B measurement matrix generated by Matlab built-in functions, which proves that the randomness of the sequence is positively correlated with the imaging quality of the measurement matrix, and also indicates the superiority of quantum cryptography used in the measurement matrix.

B. OPTIMIZE THE QUANTUM CRYPTOGRAPHY MEASUREMENT MATRIX TO RECONSTRUCT THE IMAGES

1) MATRIX ORTHOGONALIZATION PERFORMANCE TESTS

In order to further improve the imaging performance of quantum cryptography measurement matrix and verify it, we perform Schmidt orthography and numerical simulation with 32 × 32 pixels letter GI as the target object. Fig. 11 (a) is the second-order correlation imaging result of SO-QCM, and Fig. 11 (b) is the second-order correlation imaging result of QCM. As shown in Fig. 11, the reconstruction result of Schmidt orthogonalization quantum cryptography measurement matrix is greatly improved compared with that of pure quantum cryptography measurement matrix. In order to express more visually the improvement of the performance of the measurement matrix after orthogonalization, we calculated the PSNR of the corresponding reconstructed image and showed it in the lower part of the image. It can be concluded
that the PSNR value of the reconstructed image keeps rising with the increasing number of detection. For the same number of detection, the reconstructed image of SO-QCM is better than QCM.

In order to further compare the advantages and disadvantages of the measurement matrices designed in this paper, the Gaussian measurement matrix, the Schmidt orthogonalized quantum cryptography measurement matrix, and the Hadamard measurement matrix are used to reconstruct the images with the differential reconfiguration algorithms, and the reconstruction of the target object “HNU” with the size of $32 \times 32$ pixels (see Fig. 12 Object) is calculated. Where (a) represents the Gaussian random matrix reconstruction image result, (b) represents the Hadamard measurement matrix reconstruction image result, and (c) represents the orthogonalized quantum cryptography measurement matrix.
reconstruction image result. From this figure, it can be concluded that the reconstruction clarity of orthogonalized quantum cryptography measurement matrix is higher than that of Gaussian random matrix, but lower than that of samples. Relative to the traditional measurement matrix, the SO-QCM proposed in this paper has great advantages.

2) MATRIX-NORMALIZED PERFORMANCE TEST

From the previous results, we found that the quality of the orthogonalized quantum cryptography measurement matrix reconstructed image is higher than that of the Gaussian random measurement matrix, but there is a big gap with Hadamard measurement matrix. In the research process, it is found that the normalization of quantum cryptography measurement matrix will affect the final imaging quality. To further improve the performance of the quantum cryptography measurement matrix, the measurement matrix after Schmidt orthogonalization is normalized to compare the quality of the reconstructed images. The experiment used 32 × 32 pixels of “Lena” with the differential reconfiguration algorithm. Where (a) represents the Hadamard matrix reconstruction image result, (b) represents the SO-QCM reconstruction image result, (c) represents the SON-QCM reconstruction image result. As can be seen from Fig. 13, the PSNR value of the reconstructed image using the normalized SO-QCM has been greatly improved and the gap with Hadamard has been narrowed.

From the above numerical simulation results, it can be seen that QCM with good randomness can effectively reconstruct the target object. The reconstruction quality of SO-QCM processed by Schmidt orthogonalization is better than QCM. The normalized SON-QCM has better performance in reconstructing the target object.

V. CONCLUSION

In this paper, we design a remote secure CGI system based on QKD that uses quantum cryptography to achieve secure transmission and establish a new measurement matrix. The matrix was further optimized using the Schmidt orthogonalization method, which effectively improved the image reconstruction efficiency and image quality of the remote CGI system. It is found that the randomness of the sequence constituting the measurement matrix is closely related to the image reconstruction results. The QCM with a good random distribution is more efficiently reconstructed with the same number of samples, which leads to a higher imaging quality after further orthogonalization processing. This method improves the safety of the CGI system and the imaging quality on this premise, which promotes the practicality of CGI technology and provides new ideas for the application of QKD technology. Further optimization of the QCM using deep learning techniques is considered in future work to advance the reduction of sampling times and shorten the image reconstruction time with the same imaging quality.

REFERENCES

[1] Y. H. Shih, A. V. Sergienko, T. B. Pittman, D. V. Strekalov, and D. N. Klyshko, “Two-photon ‘ghost’ image and interference-diffraction,” Ann. New York Acad. Sci., vol. 755, no. 1, pp. 121–132, Apr. 1995.
[2] G. M. Gibson, B. Sun, M. P. Edgar, D. B. Phillips, N. Hempler, G. T. Maker, G. P. A. Malcolm, and M. J. Padgett, “Real-time imaging of methane gas leaks using a single-pixel camera,” Opt. Exp., vol. 25, no. 4, p. 2998, 2017.
[3] M. P. Edgar, G. M. Gibson, R. W. Bowman, B. Sun, N. Radwell, K. J. Mitchell, S. S. Welsh, and M. J. Padgett, “Simultaneous real-time visible and infrared video with single-pixel detectors,” Sci. Rep., vol. 5, no. 1, pp. 1–8, Sep. 2015.
[4] M.-Q. Yin, L. Wang, and S.-M. Zhao, “Experimental demonstration of influence of underwater turbulence on ghost imaging,” Chin. Phys. B, vol. 28, no. 9, Aug. 2019, Art. no. 094201.
[5] C.-L. Luo, W.-X. Wan, S.-Y. Chen, A.-F. Long, L.-N. Peng, S.-F. Wu, and H.-R. Qi, “High-quality underwater computational ghost imaging with shaped Lorentz sources,” Laser Phys. Lett., vol. 17, no. 10, Oct. 2020, Art. no. 105209.
[6] Y. Liu, X. Liu, L. Liu, F. Wang, Y. Zhang, and Y. Cai, “Ghost imaging with a partially coherent beam carrying twist phase in a turbulent ocean: A numerical approach,” Appl. Sci., vol. 9, no. 15, p. 3023, Jul. 2019.
[7] V. Studer, J. Bobin, M. Chahid, H. S. Mousavi, E. Candes, and M. Dahan, “Compressive fluorescence microscopy for biological and hyperspectral imaging,” Proc. Nat. Acad. Sci. USA, vol. 109, no. 26, pp. E1679–E1687, Jun. 2012.
[8] B. Sun, M. P. Edgar, R. Bowman, L. E. Vittert, S. Welsh, A. Bowman, and M. J. Padgett, “3D computational imaging with single-pixel detectors,” Sensors, vol. 14, no. 3, Apr. 2014, pp. 6134–6147, May 2014.
[9] X. Yang, L. Xu, M. Jiang, L. Wu, Y. Liu, and Y. Zhang, “Phase-coded modulation 3D ghost imaging,” Optik, Int. J. Light Electron Opt., vol. 220, Oct. 2020, Art. no. 165184.
[10] Z. Zhang, S. Liu, J. Peng, M. Yao, G. Zheng, and J. Zhong, “Simultaneous spatial, spectral, and 3D compressive imaging via efficient Fourier single-pixel measurements,” Optica, vol. 5, no. 3, p. 315, 2018.
[11] V. Durán, F. Soldevila, E. Iles, P. Clemente, E. Tajahuerce, P. Andrés, and I. Lancis, “Compressive imaging in scattering media,” Opt. Exp., vol. 23, no. 11, p. 14424, 2015.
[12] H. Yu, R. Lu, S. Han, H. Xie, G. Du, T. Xiao, and D. Zhu, “Fourier-transform ghost imaging with hard X rays,” Phys. Rev. Lett., vol. 117, no. 11, Sep. 2016, Art. no. 113901.
[13] J. H. Shapiro, “Computational ghost imaging,” Phys. Rev. A, Gen. Phys., vol. 78, no. 6, Dec. 2008, Art. no. 061802.
[14] Y. Bromberg, O. Katz, and Y. Silberberg, “Ghost imaging with a single detector,” Phys. Rev. A, Gen. Phys., vol. 79, no. 5, May 2009, Art. no. 053840.
[15] Z. Zhang, X. Wang, G. Zheng, and J. Zhong, “Hadamard single-pixel imaging versus Fourier single-pixel imaging,” Opt. Exp., vol. 25, no. 16, pp. 19619–19639, 2017.
[16] C. Zhou, X. Zhao, H. Huang, G. Wang, X. Wang, L. Song, and K. Xue, “Hadamard resolution single-pixel imaging via Hadamard ‘pipeline’ coding,” Appl. Phys. B, vol. 126, no. 10, pp. 1–10, Oct. 2020.
[17] M.-J. Sun, L.-T. Meng, M. P. Edgar, M. J. Padgett, and N. Radwell, “A Russian dolls ordering of the Hadamard basis for compressive single-pixel imaging,” Sci. Rep., vol. 7, no. 1, p. 3464, Dec. 2017.
[18] Z. Ye, H. Wang, J. Xiong, and K. Wang, “Simultaneous full-color single-pixel imaging and visible watermarking using Hadamard-bayer illumination patterns,” Opt. Lasers Eng., vol. 127, pp. 105955.1–105955.12, Apr. 2020.
[19] W.-K. Yu, “Super sub-nyquist single-pixel imaging by means of cake-cutting Hadamard basis sort,” Sensors, vol. 19, no. 19, p. 4122, Sep. 2019.
[20] S. Mendelson, A. Pajor, and N. Tomczak-Jaegermann, “Uniform uncertainty principle for Bernoulli and SubGaussian ensembles,” Constructive Approx., vol. 28, no. 3, pp. 277–289, 2008.
[21] B. I. Erkmen and J. H. Shapiro, “Signal-to-noise ratio of Gaussian-state ghost imaging,” Phys. Rev. A, Gen. Phys., vol. 79, no. 2, 2009, Art. no. 023833.
[22] J. Chen, W. Gong, and S. Han, “Sub-Rayleigh ghost imaging via sparsity constraints based on a digital micro-mirror device,” Phys. Lett. A, vol. 377, nos. 31–33, pp. 1844–1847, Oct. 2013.
[23] Z. Ye, H.-C. Liu, and J. Xiong, “Computational ghost imaging with spatiotemporal encoding pseudo-random binary patterns,” Opt. Exp., vol. 28, no. 21, p. 31167, 2020.
[24] X. Ma, “Security of quantum key distribution with realistic devices,” Rev. Mod. Phys., vol. 92, Apr./Jun. 2020.

[25] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, vol. 299, no. 5886, pp. 802–803, 1982.

[26] C. H. Bennett, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Comput., vol. 560, Dec. 2014, pp. 7–11.

[27] H. Inamori, N. Lütkenhaus, and D. Mayers, “Unconditional security of practical quantum key distribution,” Eur. Phys. J. D, vol. 41, no. 3, pp. 599–627, Mar. 2007.

[28] R. Qi, S. Zhen, Z. Lin, P. Niu, and G. L. Long, “Implementation and security analysis of practical quantum secure direct communication,” Light, Sci. Appl., vol. 8, no. 1, p. 22, 2019.

[29] B. Sun, M. P. Edgar, R. Bowman, L. E. Vittert, S. Welsh, A. Bowman, and M. J. Padgett, “Differential computational ghost imaging,” in Proc. Comput. Opt. Sens. Imag., 2013, pp. 1–3.

[30] B. Sun, S. S. Welsh, M. P. Edgar, J. H. Shapiro, and M. J. Padgett, “Normalized ghost imaging,” Opt. Exp., vol. 20, no. 15, pp. 16892–16901, 2012.

[31] C. Zhang, S. Guo, J. Cao, J. Guan, and F. Gao, “Object reconstitution using pseudo-inverse for ghost imaging,” Opt. Exp., vol. 22, no. 24, p. 30063, 2014.

[32] X. Yunru, Probabilistic Statistical Calculation Method. Tianjin, China: Nankai Univ. Press, 1994.

[33] NIST. NIST Statistical Test Suite (Version2.0), Accessed: Apr. 27, 2010. [Online]. Available: http://csrc.nist.gov/ and https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software

[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A statistical test suite for random and pseudo-random number generators for cryptographic applications,” Inf. Technol. Lab., Nat. Inst. Standards Technol., Tech. Rep. NIST Special Publication 800-22, 2001.

[35] Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” Electron. Lett., vol. 44, no. 13, pp. 800–801, Jun. 2008.

[36] B. Luo, P. Yin, L. Yin, G. Wu, and H. Guo, “Orthonormalization method in ghost imaging,” Opt. Exp., vol. 26, no. 18, p. 23093, 2018.

JIANAN WU received the Ph.D. degree in computer application technology from Jilin University, in 2013. He studied as a Visiting Scholar at the University of Ottawa, in 2015. He completed post-doctoral research with the Communication College, Jilin University, in 2017. He is currently an Associate Professor with the College of Computer Science and Technology, Changchun University. His main research interests include quantum secure communication, intelligent networks, and image processing.

YUN CHEN was born in 1996. He received the bachelor’s degree in information engineering majoring in network engineering from the Guangxi Institute of Foreign Languages. He is currently pursuing the master’s degree with the College of Network Security, Changchun University. It mainly studies quantum cryptography and ghost imaging.

CHENG ZHOU was born in 1991. He received the bachelor’s degree in physics and electrical engineering from Ningxia University, in June 2014, and the master’s degree in science from the Changchun University of Science and Technology, in 2017. He is currently pursuing the Ph.D. degree in physics with Northeast Normal University. He became an Intermediate Experimenter with the Engineering Information Engineering College, Jilin Normal University, in 2017. He has participated in many national quantum imaging academic seminars, and made a report about ghost imaging at the meeting. His main research interest includes ghost imaging.

ZHONGYANG CHEN graduated from North China Water and Hydropower University with a major in network engineering, in 2020. He is currently pursuing the master’s degree in network security with Changchun University. He learns to study ghost imaging, hyper-resolution, and noise processing, from 2020 to 2021.

CHENGQIAN XU was born in Yanting, Mianyang, Sichuan, China, in 2000. From 2018 to 2021, he studied at Changchun University. His direction of learning are image processing and quantum cryptography. His study and research is in quantum laboratories, from 2019 to 2021.

LIUJUN SONG was born in Dongfeng, Jilin, China, in 1971. He received the B.S. degree in physics education from Jilin Normal University, in 1994, the M.S. degree in theoretical physics from Jilin University, in 2003, and the Ph.D. degree in optics from the Changchun University of Science and Technology, in 2008. From 2004 to 2008, he was an Associate Professor with the Physics Department, Changchun University. From 2006 to 2007, he was a Visiting Scholar with the Physics Department, Zhejiang University. From 2009 to 2016, he was a Professor with the Physics Department, Changchun University. Since 2017, he has been a Professor with the Institute for Interdisciplinary Quantum Information Technology, Jilin Engineering Normal University. He is the author of a book and more than 50 articles. He holds three patents. His research interests include quantum information theory and application, and quantum imaging.

Prof. Song was a recipient of the Jilin Province Science and Technology Progress Award in 2011 and 2013. He is a Reviewer of the journals Optics Communications and Optics Express.

* * *