ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Proof-of-principle experimental demonstration of quantum secure imaging based on quantum key distribution

Yi-Bo Zhao(赵义博)[1,2], Wan-Li Zhang(张万里)[1,2], Dong Wang(王东)[1,2], Xiao-Tian Song(宋萧天)[1,2], Liang-Jiang Zhou(周良将)[1,2,3], Chi-Biao Ding(丁赤飚)[1,2,3]

Citation: Chin. Phys. B . 2019, 28(10): 104203 . **doi:** 10.1088/1674-1056/ab3e66
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Experimental demonstration of influence of underwater turbulence on ghost imaging

Man-Qian Yin(殷曼倩), Le Wang(王乐), Sheng-Mei Zhao(赵生妹)
Chin. Phys. B . 2019, 28(9): 094201 . **doi:** 10.1088/1674-1056/ab33ee

Mask-based denoising scheme for ghost imaging

Yang Zhou(周阳), Shu-Xu Guo(郭树旭), Fei Zhong(钟菲), Tian Zhang(张天)
Chin. Phys. B . 2019, 28(8): 084204 . **doi:** 10.1088/1674-1056/28/8/084204

Image encryption using random sequence generated from generalized information domain

Xia-Yan Zhang(张夏衍), Guo-Ji Zhang(张国基), Xuan Li(李璇), Ya-Zhou Ren(任亚洲), Jie-Hua Wu(伍杰华)
Chin. Phys. B . 2016, 25(5): 054201 . **doi:** 10.1088/1674-1056/25/5/054201

Lensless ghost imaging through the strongly scattering medium

Zhe Yang(杨哲), Lianjie Zhao(赵连洁), Xueliang Zhao(赵学亮), Wei Qin(秦伟), Junlin Li(李俊林)
Chin. Phys. B . 2016, 25(2): 024202 . **doi:** 10.1088/1674-1056/25/2/024202

Increasing the range accuracy of three-dimensional ghost imaging ladar using optimum slicing number method

Yang Xu, Zhang Yong, Xu Lu, Yang Cheng-Hua, Wang Qiang, Liu Yue-Hao, Zhao Yuan
Chin. Phys. B . 2015, 24(12): 124202 . **doi:** 10.1088/1674-1056/24/12/124202

Proof-of-principle experimental demonstration of quantum secure imaging based on quantum key distribution

Yi-Bo Zhao(赵义博)[1,2], Wan-Li Zhang(张万里)[1,2], Dong Wang(王东)[1,2], Xiao-Tian Song(宋萧天)[1,2], Liang-Jiang Zhou(周良将)[1,2,3,†], and Chi-Biao Ding(丁赤飚)[1,2,3]

[1] *National Key Laboratory of Microwave Imaging Technology, Beijing* 100190, *China*
[2] *Institute of Electronics, Chinese Academy of Sciences, Beijing* 100190, *China*
[3] *University of Chinese Academy of Sciences, Beijing* 100049, *China*

(Received 5 June 2019; revised manuscript received 15 August 2019; published online 30 September 2019)

We present a quantum secure imaging (QSI) scheme based on the phase encoding and weak+vacuum decoy-state BB84 protocol of quantum key distribution (QKD). It allows us to implement a computational ghost imaging (CGI) system with more simplified equipment and reconstructed algorithm by using a digital micro-mirror device (DMD) to preset the specific spatial distribution of the light intensity. What is more, the quantum bit error rate (QBER) and the secure key rate analytical functions of QKD are used to see through the intercept-resend jamming attacks and ensure the authenticity of the imaging information. In the experiment, we obtained the image of the object quickly and efficiently by measuring the signal photon counts with a single-photon detector (SPD), and achieved a secure key rate of 571.0 bps and a secure QBER of 3.99%, which is well below the lower bound of QBER of 14.51%. Besides, our imaging system uses a laser with invisible wavelength of 1550 nm, whose intensity is as low as single-photon, that can realize weak-light imaging and is immune to the stray light or air turbulence, thus it will become a better choice for quantum security radar against intercept-resend jamming attacks.

Keywords: quantum secure imaging (QSI), quantum key distribution (QKD), digital micro-mirror device (DMD), quantum bit error rate (QBER)

PACS: 42.30.Va, 03.67.Dd **DOI:** 10.1088/1674-1056/ab3e66

1. Introduction

How to enhance the anti-jamming ability of radar is an urgent problem to be solved in the traditional radar countermeasures technology.[1,2] In the last two decades, with the intensive research and development of the techniques of quantum communication,[3–5] quantum imaging,[6–22] and quantum radar,[23,24] a series of results have been obtained, which provide a solution for improving the anti-jamming ability of radar.

In 1995, quantum imaging was first observed,[6] also known as ghost imaging (GI). Entangled photon pairs produced by spontaneous parametric down-conversion were used, while one of the photons passing through the object was collected by a photon counter or a bucket detector with no spatial resolution (called the signal beam or object beam), its twin photon was detected by a multipixel detector [e.g., a charge-coupled device (CCD) camera] without ever passing through the object (called the reference beam). Nevertheless, by correlating the intensities measured by the bucket detector with the intensities of each pixel in the multipixel detector, an image of the object was reconstructed.[6] In a long time, entanglement swapping was considered as the necessary condition for GI.[25] However, from 2002 GI was implemented by classical light sources,[9–18] especially the groups of Wang,[12] Wu,[13] and Han[14,15] accomplished a large numbers of GI experiments based on pseudo-thermal or real thermal light sources, which proved that entanglement is not the one and only way to achieve GI. After then, computational ghost imaging (CGI) was proposed[19] and verified by experiments,[20,21] which could be deployed with only one optical beam and one detector with no spatial resolution by replacing the reference beam with a controllable and pre-modulated light source.[22] The greatly simplified imaging system reduces the number of preset patterns and the imaging computational complexity, and then raises the imaging efficiency.[22] Based on the above, CGI and quantum secure imaging (QSI) could be applied to radar imaging faultlessly. Reference [8] introduced an anti-jamming quantum radar imaging (QRI) that utilized the BB84 protocol quantum key distribution (QKD) based on polarization encoding, which could verify the authenticity of imaging information by detecting the consistency of photon polarization states between the sender and the receiver. Up to now, the BB84 protocol is the most mature and widely used quantum key distribution protocol and its theoretical security has been fully proved.[26,27] Therefore, intercept-resend attacks are exposed immediately and the authenticity of the imaging information can be guaranteed through combining the CGI and QKD on radar technology. In addition, the quantum imaging technology has many advantages of higher resolution, higher contrast, higher signal-to-noise ratio (SNR), and less influence of atmospheric turbulence[7] compared with the traditional imaging.

†Corresponding author. E-mail: ljzhou@mail.ie.ac.cn

© 2019 Chinese Physical Society and IOP Publishing Ltd

QSI will has great application value in the fields of aerial detection, military reconnaissance, and battlefield imaging in the future.

Inspired by Ref. [8], we present a QSI scheme combining the phase-encoding BB84 QKD and CGI technology. Unlike the original scheme, our scheme adopt phase-encoding QKD, in which the relative phase is rather stable against disturbance. Moreover, owing to the fact that perfect single-photon source is still unavailable, a pulsed laser source with Poisson distribution is used in the QKD system. By combing the decoy-state method, we can estimate the contribution of the multi-photon part to obtain the lower bound of QBER under the intercept-resend jamming attack, which is tighter than the origin one. In our experiment, a digital micro-mirror device (DMD) with quick response speed is used to preset the specific spatial distribution of the light intensity, and a single-photon detector (SPD) with quick response speed is used to measure the total light intensity, eventually the image of the object is retrieved through calculating the intensity distribution and the total intensity of light. Comparing with the traditional ghost imaging (TGI), QSI has been greatly improved in the data sampling rate and reduced in the imaging algorithm complexity and shortened the imaging time. More importantly, the quantum bit error rate (QBER) and the secure key rate of QKD are obtained in the experiment to see through the intercept-resend jamming attacks and ensure the authenticity of the imaging information.

2. Theory and method

The QSI system contains the imaging system and the QKD system, as shown in Fig. 1, which mainly includes a QKD sender (Alice), a QKD receiver (Bob), and the spatial light path of CGI in more details. In our scheme, Alice sends out strongly attenuated coherent states with key bits information, which is encoded into the relative phase of a pair of coherent states shifted in time that are generated by an asymmetric interferometer. These photons pass through the beam expanding lens, the obtained speckle is then modulated into a specific spatial distribution of intensity with a DMD. The pulse with certain intensity distribution illuminates the object, and is coupled into the receiver, performs the decoding and detecting procedure. Finally we can reconstruct the image of the object with the detected counts. It should be stressed that in the QKD procedure, the key bits information is encoded into the relative phase between the two time-bin mode of signal pulses, which is rather stable during the display time of one frame of the DMD, since the modulation of DMD just changes the global phase of the whole two-time-bin pulses rather than the relative phase between them. Therefore, the pulses passing through the imaging optical path and arrive at Bob without changing the coding information, and can be further correctly decoded by Bob. Compared with the conventional CGI system, the major difference is that the light source and detector are replaced by a QKD sender and receiver in our QSI scheme, with which the security of imaging can be promoted. As it is necessary to measure the photon counts and QBER during the display time of every pattern loaded in the DMD, the trigger signals of the laser, the DMD, and the SPDs should be synchronized. The image of the object is reconstructed through calculating the pre-modulated intensity distribution of the DMD and the measured total intensity of the SPDs, while the QBER is monitored to estimate whether the imaging process is safe and real.

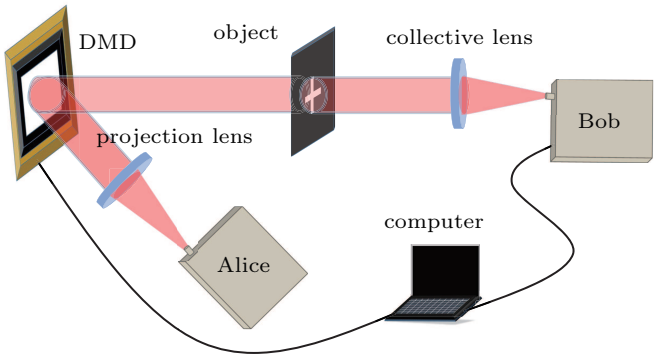


Fig. 1. Schematic of the quantum secure imaging system. Polarized single-photon from Alice passes through the beam expanding lens, is modulated into specific spatial intensity distribution by the DMD, then transmits through the object, finally is coupled into Bob and detected by SPDs. The image of the object is reconstructed and the QBER is monitored to estimate whether the imaging process is safe and real. The angle of reflection from the DMD is exaggerated in the figure for clarity but is about 24° in reality.

2.1. Quantum key distribution system

Quantum key distribution technology is one of the most mature and commonly used communication methods in quantum communication, as well as the BB84 protocol in QKD protocol, whose theoretical security has been fully proved.[26,27] So, we adopt the scheme based on the phase encoding BB84 protocol of QKD.[3,4] Our QKD system is shown in Fig. 2. It is composed of two parts of Alice and Bob. Alice uses a pulsed laser to produce coherent pulses. An intensity modulator is used to produce signal and decoy pulses of differing intensities. The vacuum pulse is produced by omitting trigger signal to the laser. An unbalanced Mach–Zehnder interferometer (UMZI) with a phase modulator (PM) in the long arm plays the role of encoder, while there is an identical UMZI in Bob.[3] SPDs are deployed by Bob to detect the interferometric outcomes from the interferometer. Moreover, an electronic variable optical attenuator (EVOA) is used to attenuate the intensity of the laser pulses to the single-photon level before sending out from the sender.[26] In the experiment, the intensities of the signal and decoy pulses are set as μ and ν to perform the weak+vacuum decoy-state BB84 QKD protocol.[28]

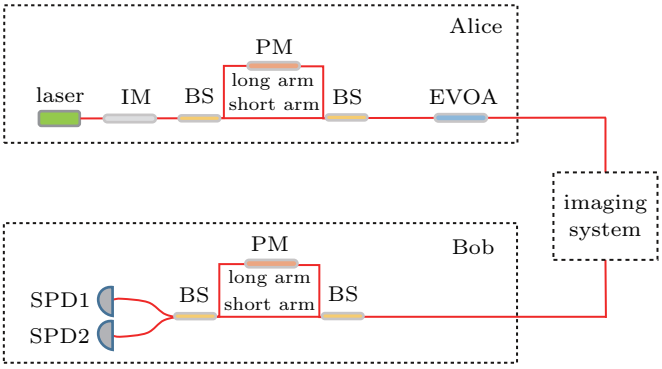


Fig. 2. Schematic of the phase encoding and weak+vacuum decoy-state BB84 protocol QKD. IM: intensity modulator; BS: beam splitter; PM: phase modulator; EVOA: electronic variable optical attenuator; SPD: single-photon detector. The signal and decoy pulses are produced by IM. Two identical UMZIs in Alice and Bob play roles of encoder. An EVOA is used to attenuate the intensity of the laser pulses to the single-photon level.

According to the phase encoding BB84 protocol, the relative phase on Alice is selected randomly from four values 0, $\pi/2$, π, and $3\pi/2$, where 0, π are in the Z basis, and $\pi/2$, $\pi/2$ are in the X basis. Bob measures the incoming quantum states from Alice also in Z or X basis randomly. Whenever Alice and Bob use the same basis, the two SPDs will get correct results with a small QBER. However, when they use different bases, the two SPDs will get an uncertain result together. Alice then reveals only whether or not the state in which she encoded that qubit is compatible with the basis announced by Bob. If the state is compatible, they keep the bit; if not, they disregard it. In this way, fifty percent of the bit string is discarded. This shorter key obtained after basis reconciliation is called the sifted key.

2.2. Intercept-resend eavesdropping strategy

In the practical QKD system, Alice uses the weak coherent source (WCS) together with the decoy-state method to substitute the unavailable single-photon source. The photon number of each pulse follows the Poisson distribution. The probability of finding an n-photon state in a pulse is given by $P_n(\mu) = \mathrm{e}^{-\mu}\mu^n/n!$, where μ is the mean photon number. With the phases randomization, the states sent by Alice are described by

$$\rho_k = \sum_{n=0}^{\infty} \frac{\mathrm{e}^{-\mu}\mu^n}{n!} |n_k\rangle \langle n_k|, \tag{1}$$

where the states $|n_k\rangle$ denote Fock states with n photons in one of the four BB84 polarization states, which are labeled with the index k, with $k = 0, \ldots, 3$ (corresponding to $0, \pi/2, \pi$, and $3\pi/2$, respectively).

In the case of quantum secure imaging or quantum radar, the potential attacker usually adopts the intercept-resend strategy to forge the target. Since the QKD system is applied to enhance its security, here we just consider the intercept-resend quantum eavesdropping strategy that was proposed by Curty *et al.*[29] Eve's attack strategy can be decomposed into three steps. In the first step, Eve obtains the total photon number n of each pulse sent by Alice via a quantum non-demolition (QND) measurement without introducing any errors. Then she performs a filter operation on the state $|n_k\rangle$ with the intention to make them distinguishable with some finite probability. Finally, in the third step, Eve measures each filtered state with the so-called square-root measurement (SRM). This measurement gives her the minimum value of the error probability when distinguishing symmetric states. After deciding which state was used by Alice, Eve needs to prepare a new signal in the state identified and gives it to Bob. The error rate introduced by Eve with this eavesdropping strategy for a signal state containing n photons is given by

$$e_n = \frac{1}{2} - \frac{\sum_{l,m=0}^{1} |\gamma_{2l}(n)\,\gamma_{2m+1}(n)|}{2\sum_{j=0}^{3} |\gamma_j(n)|^2}, \tag{2}$$

where $\gamma_j(n) = \alpha_j(n)c_j(n)$, with coefficients $\alpha_j(n)$ satisfying $|\alpha_j(n)|^2 \le 1$ for all $j = 0, \ldots, 3$ and for all $n \ge 0$. And the coefficients $c_j(n)$ satisfy $\sum_j |c_j(n)|^2 = 1$. The exact values of the coefficients $|c_j(n)|$ can be obtained explicitly as follows by using the overlaps of the four states $|n_k\rangle$ with $k = 0, \ldots, 3$:

$$\begin{aligned}
|c_0(n)| &= \sqrt{\frac{1}{4} + 2^{-(1+n/2)} \cos\left(\frac{\pi}{4}n\right)},\\
|c_1(n)| &= \sqrt{\frac{1}{4} + 2^{-(1+n/2)} \sin\left(\frac{\pi}{4}n\right)},\\
|c_2(n)| &= \sqrt{\frac{1}{4} - 2^{-(1+n/2)} \cos\left(\frac{\pi}{4}n\right)},\\
|c_3(n)| &= \sqrt{\frac{1}{4} - 2^{-(1+n/2)} \sin\left(\frac{\pi}{4}n\right)}.
\end{aligned} \tag{3}$$

For different states $|n_k\rangle$, we can obtain the minimum error rate with Eqs. (2) and (3). In the following, we calculate the case that the signal sent by Alice contains only $0 < n \le 2$ photons. In the case of single photon state $|1_k\rangle$, that is $n = 1$, from Eq. (3) we have $|c_0(1)| = |c_1(1)| = 1/\sqrt{2}$ and $|c_2(1)| = |c_3(1)| = 0$. From Eq. (2), we obtain that in this case, the partial error rate e_1 is given by

$$e_1 = \frac{1}{2} - \frac{1}{2}\frac{|\alpha_0(1)\,\alpha_1(1)|}{|\alpha_0(1)|^2 + |\alpha_1(1)|^2}. \tag{4}$$

It is easy to get the minimum value of $e_1 = 0.25$ for all $|\alpha_j(1)|^2 \le 1$.

The analysis for the case of $n = 2$ is similar. The coefficients $c_j(2)$ of the signal states $|2_k\rangle$ are of the forms $|c_0(2)| = |c_2(2)| = 1/2$, $|c_1(2)| = 1/\sqrt{2}$, and $|c_3(2)| = 0$, respectively. The partial error rate e_2 is given by

$$e_2 = \frac{1}{2} - \frac{1}{\sqrt{2}}\frac{|\alpha_0(2)\,\alpha_1(2)| + |\alpha_1(2)\,\alpha_2(2)|}{|\alpha_0(2)|^2 + 2|\alpha_1(2)|^2 + |\alpha_2(2)|^2}. \tag{5}$$

Then we can obtain the minimum value of $e_2 = \left(2-\sqrt{2}\right)/4 \approx 0.146$.

In order to give the lower bound of total error rate of the signal state at the present of intercept-resend attack, we adopt the model of decoy-state method to estimate the yield of photon pulses.[28] In the weak+vacuum decoy-state method, Alice randomly prepares the signal, decoy, and vacuum state with intensities of μ, ν, and 0, respectively. For $0 < \nu < \mu \leq 1$, the following inequalities hold for all $n \geq 3$:

$$\frac{P_n(\mu)}{P_n(\nu)} \geq \frac{P_3(\mu)}{P_3(\nu)}, \quad P_1(\mu) > P_1(\nu), \quad P_2(\mu) > P_2(\nu). \tag{6}$$

The overall gains of the signal and decoy state are given by

$$Q_\mu = \sum_{n=0}^{\infty} P_n(\mu) Y_n, \quad Q_\nu = \sum_{n=0}^{\infty} P_n(\nu) Y_n, \tag{7}$$

where Y_n is the yield of an n-photon state, i.e., the conditional probability of a detection event at Bob's side given that Alice sends out an i-photon state.

By using the inequalities (6) and Eq. (8), the joint contribution of one-photon and two-photon components can be deduced as follows:

$$P_1(\nu) Y_1 + P_2(\nu) Y_2 \geq \frac{P_3(\mu) Q_\nu - P_3(\nu) Q_\mu - [P_0(\nu) P_3(\mu) - P_0(\mu) P_3(\nu)] Y_0}{P_3(\mu) - P_3(\nu)}, \tag{8}$$

where Y_0 is the background rate, which includes the detector dark count and other background contributions such as the stray light from timing pulses.

The total error rate of the decoy state when Eve performs the intercept-resend attack is given by

$$E_\nu Q_\nu = \sum_{i=0}^{\infty} e_i P_i(\nu) Y_i = e_0 P_0(\nu) Y_0 + e_1 P_1(\nu) Y_1 + e_2 P_2(\nu) Y_2 + \sum_{i=3}^{\infty} e_i P_i(\nu) Y_i \geq P_0(\nu) Y_0/2 + e_2 [P_1(\nu) Y_1 + P_2(\nu) Y_2], \tag{9}$$

where e_i is the error rate of the i-photon state, and the error rate of the background $e_0 = 1/2$. Thus we can obtain the lower bound of the decoy state total error rate

$$E_\nu^{\mathrm{L}} = \left[\frac{1}{2} P_0(\nu) Y_0 + e_2 \frac{P_3(\mu) Q_\nu - P_3(\nu) Q_\mu - [P_0(\nu) P_3(\mu) - P_0(\mu) P_3(\nu)] Y_0}{P_3(\mu) - P_3(\nu)}\right] \Big/ Q_\nu. \tag{10}$$

Therefore, one can monitor the error rate of the decoy state, when the error rate of our QSI system is greater than E_ν^{L}, it implies the existence of Eve and the images obtained from a signal cannot be considered secure. In addition, whether our QKD system obtains secure keys can also be a criterion of secure imaging.

2.3. Computational quantum imaging system

CGI is an improvement from TGI. A spatial light modulator (SLM) or a CCD is used to preset the specific spatial distribution of the light intensity. Disregarding the reference beam, so just a single-pixel detector is needed.[20] In this imaging scheme, take the DMD to be a part of Alice. According to the security requirement of the decoy state BB84 protocol, the intensity of the laser pulses has to be lowered to the single-photon level at the exit of the DMD by an EVOA.

As in our scheme, a DMD is used to preset intensity patterns of speckles, and single-photon detectors are employed to measure the counts corresponding to each pattern. Suppose N is the number of intensity patterns modulated by the DMD, one can obtain the total count B_i $(1 \leq i \leq N)$ during the display time of the i-th pattern, whose intensity distribution is denoted by $I_i(x,y)$ $(1 \leq i \leq N)$. Then the image of the object can be obtained by summing the calculated intensities I_i with the appropriate weights B_i[20]

$$O(x,y) = \frac{1}{N} \sum_{i=1}^{N} (B_i - \langle B_i \rangle) [I_i(x,y) - \langle I_i(x,y) \rangle], \tag{11}$$

where

$$\langle B_i \rangle = \frac{1}{N} \sum_{i=1}^{N} B_i \tag{12}$$

is the mean value of B_i, and B_i meets the following formula:

$$B_i \propto \iint T(x,y) I_i(x,y), \tag{13}$$

where $T(x,y)$ is the transmission function of the object.

3. Experiment and results

The QSI system is set up as shown in Fig. 3. In the QKD system, the pulsed laser is working at a frequency of 40 MHz and a central wavelength of 1550.12 nm. The SPD is working at Geiger mode and has a detection efficiency of 10% for photons. The intensities of the signal, decoy, and vacuum state are set to $\mu = 0.68$, $\nu = 0.18$, and 0 with the probabilities of 13/16, 2/16, and 1/16, respectively. In the quantum imaging part, the array of the DMD micro-mirrors (G4100 from TI, the control board is made by x-digit) is 1024×768, and the size of every micro-mirror (one pixel) is 13.68 μm×13.68 μm. Since

each micro-mirror is so small that the laser energy reflected from it is extremely low, a new array of 24×24 pixels is re-selected and controlled with the same state in any case. The size of the new block is approximately 328.32 μm×328.32 μm when ignoring the gaps between the micro-mirrors. We choose only the square areas wherever covered by the light spot and the intensity is adequate enough. So, the DMD is divided into $20 \times 20 = 400$ blocks, Figure 4 shows the simplest binary pattern loaded into the DMD that only one block is in the "on" state and the others are in the "off" state. In all the binary patterns, each block appears just only once, which is similar to spot scanning. In this way, only 400 binary patterns are needed, which can reduce the complexity of the imaging algorithm and greatly save the imaging time.

After completing the connection of experimental devices as shown in Fig. 3, set up the frames number $N = 400$ and frame frequency $f = 200$ Hz. Run the DMD in the fully open mode, and make the QKD work normally through scanning, and set up every parameter within QKD before placing the object. Then, put the "+" type object into this system, and load 400 random binary patterns into the DMD. Run the whole system synchronously. The signal photon counts and QBER are measured during the display time of each pattern frame. The corresponding results of the QKD procedure are shown in Table 1, which are obtained by following the standard decoy-state BB84 QKD protocol. According to Eq. (11), the reconstructed image of the object is shown in Fig. 5. The SNR is 23 dB, where SNR is defined as $\mathrm{SNR} = \bar{s}^2/\sigma_n$, $\bar{s}$ is the average of the signal intensity, and σ_n is the variance of the background intensity. The difference between the average intensities of the bright and dark regions of the images is regarded as the signal, and the variation of dark background is considered as the noise.[22,30] The lower bound of the error rate is calculated to be 14.51% according to Eq. (10), and a secure key rate of 571.0 bps is achieved during the imaging period.

As can be seen from Table 1 and Fig. 5, the image information of the object can be obtained by using the QSI scheme, and the average QBER is 3.99%, which is below the lower bound and proves that the imaging process is safe and real. Once the jammer of object tries to carry out the intercept-resend strategy, it is bound to lead to the over threshold increase of QBER under the premise of presence of photon counts. In general, we think that the jammer of object has carried on the intercept-resend strategy and the imaging is no longer safe and real when the average of QBER is higher than 14.51%. Therefore, our QSI system can be used as quantum secure radar against jammers.

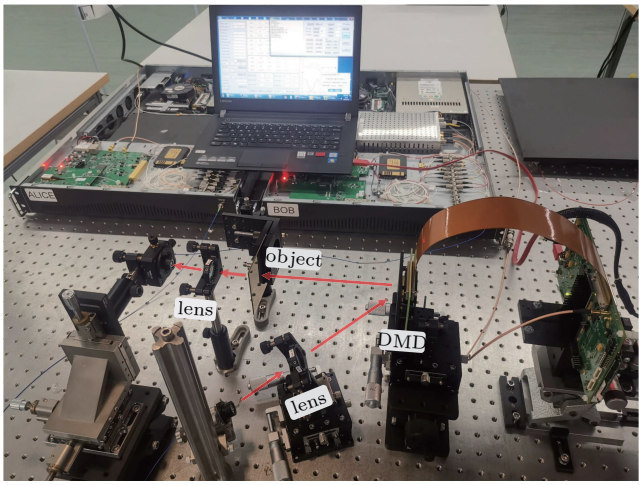


Fig. 3. Experimental setup of the QSI system. The red arrows indicate the path of light roughly.

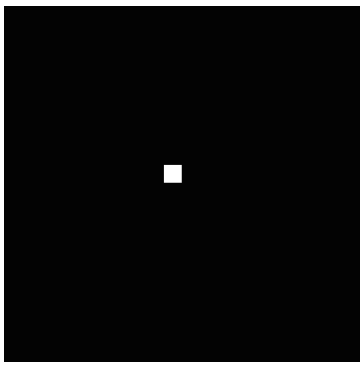


Fig. 4. The simplest binary pattern loaded into the DMD that only one block is in the on state and the others are in the off state.

Table 1. Experimental results of QKD procedure.

Q_μ	Q_ν	Y_0	E_μ	E_ν
2.69×10^{-4}	7.32×10^{-5}	3.0×10^{-6}	2.13%	3.99%

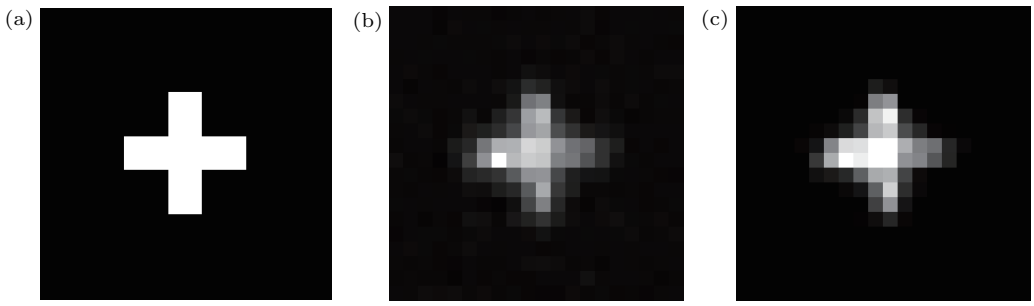


Fig. 5. Results of numerical simulation and QSI experiment of a "+" type object. (a) The result of numerical simulation of imaging the object according to Eq. (11). (b) The result of using the measured signal intensity distribution for imaging the object directly. (c) The result of calculating the measured signal intensity and the presetting intensity distribution for imaging the object according to Eq. (11), which is better than (b).

At the same time, we can see that the image resolution is not high. The main reason is the serious diffraction effect of the DMD. As we know, the DMD is composed of many micro mirrors, which is similar to a two-dimensional diffraction grating. It has a strong diffraction effect on monochromatic light, and becomes stronger with the increase of the wavelength,[31] which can hardly even be used for imaging in the mid-infrared band. Therefore, even if all the micro mirrors of the DMD keep in the off state, the detector will still measure much energy due to the diffraction effect, which will greatly reduce the SNR and the imaging quality. As a result, neither the new block of the binary patterns can be too small, otherwise the diffraction noise will drown out the signal energy which makes the SNR relatively low. Nor the new block can be too large, otherwise the imaging resolution will be dissatisfactory. Therefore, it is necessary to find a balanced block in the experiment that makes the imaging quality best. In our experiment, the block with size of 328.32 μm×328.32 μm is relatively appropriate. In addition, we can minimize the diffraction effect by the following three methods. Firstly, we can change the distribution of the diffraction spots and energy by adjusting the incident angle of light on the DMD to minimize the diffraction effect. Secondly, we can increase the distance between the DMD and the detector to reduce the diffraction effect, because the diffraction spots are distributed at some certain angles. The farther away the distance, the larger deviation of the diffraction spots, and the less stray light coupled into the detector. Finally, we can design the wavelength of the light to match the DMD to reduce the diffraction effect, but all the devices need to be matched to this wavelength, such as the DMD, the laser, and the detector of QKD, which is a troublesome and complex thing. In the future works, we will focus on the research how to reduce the diffraction effect of DMD to make the imaging quality optimal.

4. Conclusion

We propose a QSI scheme based on the phase encoding and weak+vacuum decoy-state BB84 protocol QKD that can resist the intercept-resend strategy of the jammers. The authenticity and safety of the imaging process are ensured by the theoretical unconditional security of QKD, and the QBER and the secure key rate analytical functions of QKD are used to estimate whether the jammer of object carries out the intercept-resend attacks. In our experiment, we obtain a secure key rate of 571.0 bps and a secure average QBER of 3.99%, which is below the lower bound of 14.51%. In the imaging system, we synthetically use the CGI scheme, SPDs and DMD both with faster response speed that greatly improve the imaging efficiency. This scheme is suitable for both objects with transmission or reflection. Furthermore, the system uses a WCS with invisible wavelength of 1550 nm, which can realize weak-light imaging and be immune to the stray light or air turbulence. Thus, it will become a better choice for quantum secure radar against jammers. But at the same time, it is undeniable that the more obvious diffraction effect of the DMD on the longer wavelength light will reduce the imaging SNR and quality. We believe that the diffraction effect can be minimized and the imaging quality can be improved by continuously adjusting the incident angle of light on the DMD, increasing the distance between the DMD and the detector, or designing the wavelength of the light to match the DMD.

Acknowledgment

We acknowledge Xiaoming Lu, Di Jiang, and Bin Chen for fruitful discussions and software support.

References

[1] Zhang J D, Zhu D Y and Zhang G 2013 *IEEE Trans. Aerosp. Electron. Syst.* **49** 1290
[2] Butt F A, Naqvi I H and Najam A I 2012 *Proceedings of* 2012 15*th International Multitopic Conference (INMIC)*, December 13–15, 2012, Islamabad, Pakistan, p. 137
[3] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[4] Zhao Y, Qi B, Ma X F, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[5] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[6] Pittman T B, Shih Y H, Strekalov D V and Sergienko A V 1995 *Phys. Rev. A* **52** R3429
[7] Zhang P L, Gong W L, Shen X and Han S S 2010 *Phys. Rev. A* **82** 033817
[8] Malik M, Maga?na-Loaiza O S and Boyd R W 2012 *Appl. Phys. Lett.* **101** 241103
[9] Bennink R S, Bentley S J and Boyd R W 2002 *Phys. Rev. Lett.* **89** 113601
[10] Gatti A, Brambilla E, Bache M and Lugiato L A 2004 *Phys. Rev. Lett.* **93** 093602
[11] Valencia A, Scarcelli G, D'Angelo M and Shih Y H 2005 *Phys. Rev. Lett.* **94** 063601
[12] Xiong J, Cao D Z, Huang F, Li H G, Sun X J and Wang K G 2004 *Phys. Rev. Lett.* **94** 173601
[13] Zhang D, Zhai Y H, Wu L A and Chen X H 2005 *Opt. Lett.* **30** 2354
[14] Cheng J and Han S S 2004 *Phys. Rev. Lett.* **92** 093903
[15] Zhang M H, Wei Q, Shen X, Liu Y F, Liu H L, Chen J and Han S S 2007 *Phys. Rev. A* **75** 021803
[16] Si Y, Kong L J, Li Y N, Tu C H and Wang H T 2016 *Chin. Phys. Lett.* **33** 034203
[17] Li H X, Bai Y F, Shi X H, Nan S Q, Qu L J, Shen Q and Fu X Q 2017 *Chin. Phys. B* **26** 104204
[18] Luo B, Wu G H and Yin L F 2018 *Chin. Phys. B* **27** 094202
[19] Shapiro J H 2008 *Phys. Rev. A* **78** 061802
[20] Bromberg Y, Katz O and Silberberg Y 2009 *Phys. Rev. A* **79** 053840
[21] Katz O, Bromberg Y and Silberberg Y 2009 *Appl. Phys. Lett.* **95** 131110
[22] Khamoushi S M M, Nosrati Y and Tavassoli S H 2015 *Opt. Lett.* **40** 3452
[23] Shapiro J H 2007 *Proceedings of SPIE* 6603 *Noise and Fluctuations in Photonics, Quantum Optics, and Communications*, June 7, 2007, Florence, Italy, p. 660306
[24] Jiang K B, Lee H, Gerry C C and Dowling J P 2013 *J. Appl. Phys.* **114** 193102
[25] Abouraddy A F, Saleh B E A, Sergienko A V and Teich M C 2001 *Phys. Rev. Lett.* **87** 123602
[26] Lo H K and Chau H F 1999 *Science* **283** 2050
[27] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[28] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[29] Curty M and Lütkenhaus N 2005 *Phys. Rev. A* **71** 062301
[30] Bai B, He Y C, Liu J B, Zhou Y, Zheng H B, Zhang S L and Xu Z 2017 *Optik* **147** 136
[31] Dupuis J R and Mansur D J 2012 *Proceedings of Emerging Digital Micromirror Device Based Systems and Applications IV*, February 13, 2012, San Francisco, California, United States, p. 82540J