Quantum secure ghost imaging

Xin Yao,[1,2] Xu Liu,[1,2] Lixing You,[3] Zhen Wang,[3] Xue Feng,[1,2] Fang Liu,[1,2] Kaiyu Cui,[1,2] Yidong Huang,[1,2] and Wei Zhang[1,2,*]

[1]*Beijing National Research Center for Information Science and Technology (BNRist), Beijing Innovation Center for Future Chips, Electronic Engineering Department, Tsinghua University, Beijing 100084, China*

[2]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*

[3]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

(Received 10 September 2018; published 10 December 2018)

In this work, we propose a scheme of quantum secure ghost imaging (QSGI), which combines temporal quantum ghost imaging and security test based on quantum entanglement. Utilizing the quantum feature of entangled photon pairs, the eavesdropping in the imaging process can be detected, with a certain degree of protection on the object information. The proposed scheme is demonstrated by experiment, in which photon pairs are generated by a quantum light source based on a silicon waveguide. Two-dimensional patterns are imaged line by line over 50 km optical fibers and the security test is realized by two-photon interference for energy-time entanglement. QSGI could be applied in scenarios of secure imaging and surveillance, and may inspire new ideas on specific quantum communication tasks.

DOI: 10.1103/PhysRevA.98.063816

I. INTRODUCTION

Ghost imaging features a way of indirect imaging by the correlation measurement of two beams and this intriguing technique has attracted intensive attention over the past two decades [1]. The first quantum ghost imaging experiment was realized by photon pairs generated by spontaneous parametric down conversion (SPDC) in nonlinear crystals [2]. The momentum-momentum correlation was utilized to realize imaging in a nonlocal manner. After that, the concept of ghost imaging has been deeply developed "from quantum to classical to computational" [3-8], with schemes of thermal ghost imaging [3], computational ghost imaging [4], compressive ghost imaging [5], and so on. Traditionally, quantum ghost imaging depends on the position-position or momentum-momentum correlation of photon pairs, which cannot be distributed in optical fibers. Recently, quantum ghost imaging over optical fiber is realized by utilizing frequency correlation of photon pairs [9] since the frequency correlation can be well maintained during the distribution of photon pairs over optical fibers. It was named as temporal ghost imaging since it was realized by the time-resolved coincidence measurement.

Typically, in the ghost imaging scheme, the signal beam passing through the object is collected by a single-pixel detector (without spatial resolution) while the multipixel detector is placed in another spatially separated beam, i.e., a test beam. Consequently, neither signal beam nor test beam can singly image the object. The feature of ghost imaging provides possibilities on realizing secure imaging between the two parties. In the computational version, the test beam and the multipixel detector can be removed by transmitting the laser source through a spatial light modulator (SLM) [4]. Based on that, a technique of optical security was developed in which the inputs of SLM are shared secret keys between legal users and the outputs of single-pixel detector are treated as the ciphertext [10–12]. The eavesdropper cannot retrieve the object information if he only obtains the ciphertext. On the other hand, quantum key distribution (QKD), as the best-known technology of quantum cryptography, can proffer new ideas and operations for the secure imaging. In recent years, QKD over optical fibers of several hundred kilometers [13,14] and over free-space links of thousands of kilometers by satellite [15–17] have been realized. Additionally, commercial secure communication systems based on QKD also began to emerge in the past decade. Based on QKD technology, many novel protocols for specific communication tasks were explored and demonstrated in recent years, such as quantum digital signature [18,19], quantum coin flipping [20], quantum money [21,22], and multiuser communication networks [23,24]. Furthermore, the advantage of QKD against potential perturbation can also be applied in other optical techniques. An interesting scheme was proposed by Boyd *et al.* [25] where they extended the BB84 protocol of QKD to an active imaging system against intercept-resend jamming from the imaging object like a stealth aircraft.

In this work, we propose and demonstrate a scheme of quantum secure ghost imaging (QSGI) against intercept-resend eavesdropping over the long-distance transmission link in the imaging process. QSGI combines temporal ghost imaging and security test based on the entanglement protocol of QKD [26,27]. First, the principle and protocol of QSGI are introduced, and then a theoretical analysis on its security is provided. Finally, the scheme is demonstrated by experiment, in which broadband energy-time entangled photon pairs are generated by a quantum light source based on a silicon waveguide and the length of transmission fibers is 50 km. The analysis of signal-to-noise ratio (R_{SN}) shows that our

*zwei@tsinghua.edu.cn

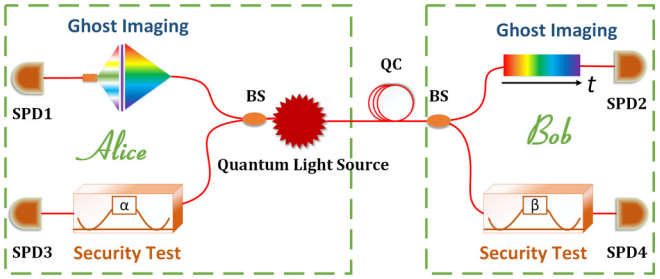

FIG. 1. The schematic of QSGI. SPD, single photon detector; BS, beam splitter; QC, quantum channel.

proposed scheme can provide a certain degree of protection on the object information in the imaging process.

II. QSGI PROTOCOL

The schematic diagram of QSGI is shown in Fig. 1. It is based on a telecom-band quantum light source, which generates energy-time entangled photon pairs. It could be realized by spontaneous parametric down-conversion [28] or four wave mixing [29] under continuous wave (CW) pumping. In the QSGI scheme, Alice holds the quantum source with broadband joint spectral density of the biphoton state. She keeps signal photons and sends idler photons to Bob over optical fibers.

The proposed QSGI realizes two functions simultaneously, which are quantum temporal ghost imaging and security test protecting the ghost imaging process. At Alice's side, signal photons of photon pairs are randomly directed to two single photon directors (SPD1 and SPD3) by a beam splitter (BS). Similarly, idler photons at Bob side are randomly directed to SPD2 and SPD4 by another BS. The temporal ghost imaging is based on the coincidence measurement of SPD1 and SPD2. At Alice's side, before the signal photons are detected by SPD1, they are dispersed to different directions by the spatial dispersion component such as a grating, and then they illuminate the object, recording the spatial information of the object on their spectrum. The transmitted (or reflected) signal photons are detected by SPD1 without spatial or frequency resolution. At Bob's side, a temporal dispersion component before SPD2 is used to diffuse arrival times of the idler photons according to their frequencies. In this way, the frequency correlation of signal-idler photons is transformed to the correlation between the spatial positions of the signal photons at Alice and the arrival times of the idler photons at Bob. By this correlation, quantum temporal ghost imaging is realized. Furthermore, the part of object illumination with a spatial dispersion component at Alice's side could be equivalently replaced by a programmable optical filter. The pattern of the filtering spectrum could also act as the object information to be transmitted. Continuous information transmission could be realized by successively programming the pattern. On the other hand, the function of the security test is based on the coincidence measurement of SPD3 and SPD4. The property of energy-time entanglement in the photon pairs is checked in the security test, which can be performed by the Franson-type interference similar to those in entanglement-QKD schemes [26,27]. The perturbation on the quantum channel would lead to the decrease of fringe visibility of the two-photon interference, which can indicate the eavesdropping fraction and provide a certain degree of protection on the ghost imaging process.

The protocol of QSGI integrates temporal ghost imaging and security test together and basically has six steps.

(1) Clock synchronization between Alice and Bob, by which the measurement time is equally divided into many time bins. The time bins are numbered at both sides.

(2) Photon pairs are generated by the quantum light source. For each time bin, no more than one pair appears. Signal photons are kept at Alice and idler photons are sent to Bob by a fiber link.

(3) Alice and Bob take the single photon detections for temporal ghost imaging and security test, respectively. The timing information of each detection events at both sides is recorded. Since the temporal dispersion component for ghost imaging disperses the arrival times of broadband idler photons at Bob's side, the time bins should be large enough to ensure that most of the photon pairs arrive at the same bins at both sides.

(4) Bob sends his security-test records to Alice through a classical channel, by which Alice constructs the fringe of the two-photon interference and checks the degradation of fringe visibility (ΔV).

(5) Bin sifting. By the classical channel Bob tells Alice the numbers of time bins in which he detects the idler photons for temporal ghost imaging. Alice checks her photon records and selects those in the time bins declared by Bob, abandoning other single photon events.

(6) According to the fringe degradation ΔV, Alice calculates the data size of photon records from ghost-imaging detector after bin sifting, and sends those records to Bob by the classical channel. Bob could retrieve the image by the coincidence measurement of photons' arrival times.

According to the protocol, since Alice only sends her records in the time bins declared by Bob, these records are useless for the potential eavesdropper (Eve) if he simply intercepts some photons by the beam splitter over the quantum channel. Hence the intercept-resend strategy is reasonable and practical for Eve. However, due to the quantum no-cloning theorem, the intercept-resend attack would degrade the quantum entanglement of photon pairs, which could be checked by the security test. Assuming that under a trusted condition excluding any eavesdropper's intrusion, the fringe visibility of the two-photon interference is V_0, which can be measured in the system calibration. Supposing the existence of Eve over the quantum channel, he would intercept a fraction of idler photons, which is denoted by x, and resend the fake photons to Bob. The intercept-resend attack would bring the perturbation into the interference measurement, leading to a degradation of ΔV. Theoretical analysis (see Appendix) shows that the fraction of intercept-resend photons can be calculated by

$$\Delta V = x V_0. \tag{1}$$

On the other hand, the quality of ghost imaging could be represented by its R_{SN} [30,31]. The image's R_{SN} at Bob depends on the data size of photon records Alice sends to Bob. It can be indicated by the measurement time for these records, which is

denoted by t. Theoretical analysis shows that if the object is a mask with binary transmission levels (the transmission $T = 0$ or 1 at each pixel in the pattern) and the coincidence counts at different pixels satisfy the Poisson distribution, the R_{SN} of the image at Bob's side can be expressed as

$$R_{SN\,\mathrm{Bob}} = \sqrt{\frac{\xi_{\mathrm{CAR}} - 1}{\xi_{\mathrm{CAR}} + 1} \frac{R\eta_{\mathrm{A}}\eta_{\mathrm{B}}}{k} t}, \tag{2}$$

where ξ_{CAR} is the coincidence-to-accidental coincidence ratio of temporal ghost imaging; R is the generation rate of photon pairs from the quantum light source; η_{A} and η_{B} are collection efficiencies of signal-idler photons for ghost imaging at Alice and Bob, respectively; k is the horizontal pixel number of the image.

If Eve performs the eavesdropping by the intercept-resend strategy, he could also make the coincidence measurement by the data Alice sends to Bob over the classical channel and the timing information of the idler photons he has intercepted over the quantum channel. Since the intercept-resend fraction is x, it can be expected that after the time-bin sifting, the ratio of the coincidence counts at Eve and Bob is also x, leading to

$$R_{SN\,\mathrm{Eve}} = \sqrt{x}\, R_{SN\,\mathrm{Bob}}. \tag{3}$$

It can be seen that the R_{SN} of the image at Eve is always lower than that at Bob since x is always lower than 1. For a specific set of patterns, such as letters of an alphabet, the R_{SN} criterion can be defined and one cannot recognize the ghost image with R_{SN} not higher than the criterion. According to Eqs. (2) and (3), Alice can control the R_{SN} of Eve's image and make it not higher than the criterion by limiting the photon records she sends to Bob through the classical channel. Meanwhile, the data size from Alice should be large enough to make Bob's R_{SN} higher than the criterion, realizing the imaging from Alice to Bob. The security of QSGI is realized by this way. The details of the theoretical analysis of Eqs. (1) to (3) are shown in the Appendix.

III. EXPERIMENTAL DEMONSTRATION

Next, we experimentally demonstrate the principle of QSGI and the setup is illustrated in Fig. 2. At Alice, energy-time entangled photon pairs are generated by the spontaneous parametric four-wave mixing in a silicon waveguide under CW pumping of 1530.33 nm (linewidth less than 100 kHz, N7714A, Keysight Technologies). The waveguide, with a cross-section size of 500 × 220 nm and a length of 1 cm, is coupled with optical fibers through a vertical-coupling grating on the waveguide and the insertion loss of the sample is ∼16 dB. The broadband signal (idler) photons generated in the waveguide are filtered by cascaded coarse wavelength division multiplexers (CWDMs) with a central-wavelength of 1550 nm (1510 nm) and bandwidth of ∼16 nm. The signal photons are left at Alice and directed into two paths by a 50:50 fiber coupler. In one path, the photons are used to perform the security test based on the Franson-type interference. They pass through an unbalanced Mach-Zender Interferometer (UMZI) with 400-ps arm-length difference, and then they are detected by a superconducting nanowire single photon detector (SNSPD) [32]. The phase difference

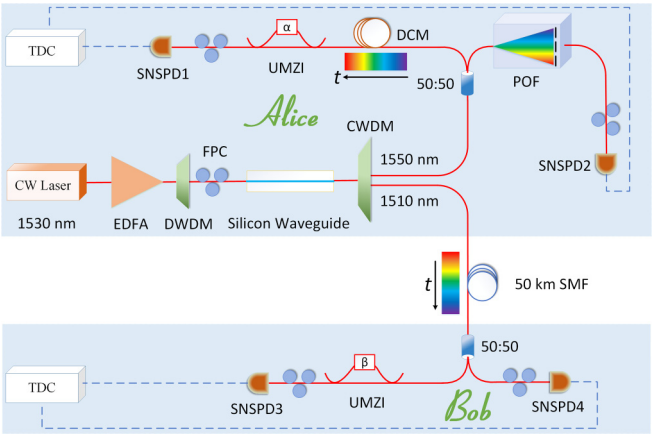

FIG. 2. Experimental setup. Energy-time-entangled photon pairs are generated by spontaneous four-wave mixing in a silicon waveguide. Signal photons are kept at Alice and idler photons are sent to Bob through single-mode fibers of 50 km. At both sides, photons are randomly directed to perform the security test and quantum temporal ghost imaging. 50:50: fiber coupler; EDFA: Erbium doped fiber amplifier; FPC: fiber polarization controller; DWDM: dense wavelength division multiplexer; CWDM: coarse wavelength division multiplexer; POF: programmable optical filter (WaveShaper); SMF: single-mode fiber; DCM: dispersion compensation module; UMZI: unbalanced Mach-Zehnder interferometer; SNSPD: superconducting nanowire single-photon detector; TDC: time-to-digital converter.

between the two arms of the UMZI can be adjusted by controlling the voltage on it. The signal photons in the other path are spectrally modulated by the programmable optical filter (WaveShaper 1000A, Finisar Corp.), and then detected by another SNSPD. It is worth noting that the filter is based on a spatial grating and spatial light modulator, which is similar to the object illumination part shown in Fig. 1. Meanwhile, idler photons are sent to Bob through single-mode fibers of 50 km. They are also separated by a 50:50 fiber coupler into two paths. Some idler photons are randomly directed into the security-test path. For compensating the group velocity dispersion (GVD) of the fiber link (∼700 ps/nm), a dispersion compensation module (DCM) is inserted before the UMZI at Alice, by which the nonlocal dispersion cancellation [33,34] is realized for measuring the Franson-type interference fringe of the energy-time entanglement. In the other path, the idler photons are utilized to realize quantum temporal ghost imaging. The GVD introduced by long-distance fibers disperses the arrival times of the broadband idler photons to ∼10 ns. Thus, spectrum patterns modulated by the WaveShaper can be ghostly imaged with the time-domain coincidence measurement of Alice's signal photons through the WaveShaper and Bob's idler photons through the long-distance transmission fibers. Four NbN superconducting nanowire single photon detectors (SNSPD) are used in the experiment with detection efficiencies at 1550 nm of ∼50%, dark-count rates of ∼200 Hz, and timing jitters of ∼70 ps (full-width at half-maximum). Single photon events are precisely recorded in the free-running mode by time-digital converters (PicoQuant HydraHarp 400).

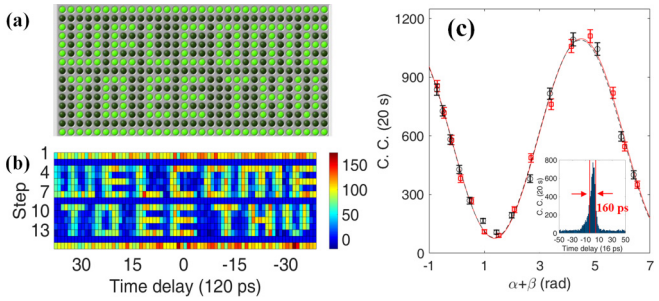

FIG. 3. A typical result of QSGI. (a) The imaging pattern set by the programmable optical filter. (b) The image at Bob retrieved by QSGI. (c) The visibility of the Franson-type interference for security test, indicated by the red squares, is 86.9% ± 2.6%. The inset shows a typical coincidence peak by nonlocal dispersion cancellation. The result of back-to-back measurement without single-mode fibers and DCM is performed (black circles) for comparison, with a visibility of 86.4% ± 2.7%. C. C., coincidence count.

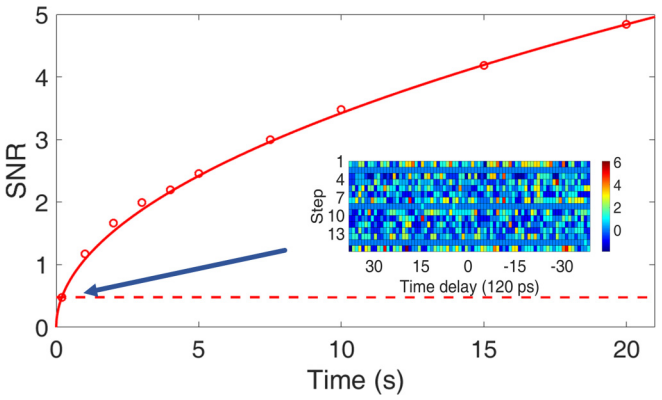

FIG. 4. R_{SN} of Bob's image versus data size (time) of photon records Alice sends to Bob. The circles are calculated R_{SN} according to experimental results. The fitting curve is $R_{SN} = 1.07\sqrt{t}$ according to Eq. (2). The R_{SN} criterion is set as 0.48 (fitting value), indicated by the dashed line. By this criterion, the data size for retrieving a recognizable image is $t > 0.2$ s. The inset shows the ghost image with $t = 0.2$ s.

A. Ghost imaging

At Alice 'sside, the object is a two-dimensional pattern with 31 × 15 pixels, shown in Fig. 3(a). Green (black) pixels in the pattern indicate that photons with corresponding frequencies can pass through (be blocked by) the programmable optical filter. The pixels in the first and last lines are all transmitted for the R_{SN} calculation of the image constructed by quantum temporal ghost imaging. The pattern is imaged line by line in 15 steps of QSGI. In each step, a line of the pattern (31 pixels) is encoded on the spectrum of signal photons (1544–1558 nm) by the programmable optical filter. The photon count rate of Alice's SNSPD2 for temporal ghost imaging is 465 kHz when the programmable optical filter is set that all the signal photons can pass through, and that of Bob's SNSPD4 is 208 kHz. The coincidence count rate $R\eta_A\eta_B \approx 400$/s and therefore, the generation rate of photon-pair R in the silicon waveguide is 8×10^7 pair/s with collection efficiencies $\eta_A = -25$ dB and $\eta_B = -28$ dB. Alice and Bob collect these photons for 20 s and obtain a coincidence histogram, which retrieves one line of the pattern. The imaging process totally takes 5 min and the ghost image is shown in Fig. 3(b), where the average accidental coincidence count is subtracted in each line for the better visual effect. The temporal range of the coincidence measurement is ∼10 ns, which is determined by the bandwidth of idler photons and the GVD introduced by the single-mode fibers of 50 km, and the horizontal pixel number $k = 78$ with the temporal resolution of 120 ps. The coincidence-to-accidental coincidence ratio ξ_{CAR} is 1.44 in the temporal ghost imaging. It can be seen that the image is clear under a measurement time of 20 s for each line. It should be noted that the time-bin sifting is performed before the coincidence processing as the step (5) of the protocol requires. The bin size is set as 0.2 μs, which is one order of magnitude smaller than the average time intervals of single photon events at both sides and one order larger than the temporal range of the coincidence measurement, ensuring most of photon pairs are in the same time bins. If there are two or even more single photon events in one time bin, such records are abandoned and the possibility is less than 2.5%.

B. Security test

The security test is realized by the Franson-type interference, using the coincidences of the single photon events recorded by SNSPD1 and SNSPD3. The measured interference fringe is shown in Fig. 3(c), in which the inset shows a typical measured coincidence peak. It can be seen that the full width at half height of the coincidence peak is narrowed to 160 ps by nonlocal cancellation of dispersion. Hence the three coincidence peaks in Franson-type interference measurement can be discriminated effectively when the UMZIs with 400-ps arm-difference are used in the experiment. The result of the Franson-type interference is indicated by the red squares, with a raw visibility of 86.9% ± 2.6%. On the other hand, the result of the back-to-back measurement is also shown by black circles for comparison, in which long-distance single-mode fibers and DCM are replaced by variable optical attenuators with the same attenuations, respectively. The visibility of the back-to-back result is 86.4% ± 2.7%, which can be viewed as the calibration value under trusted condition (V_0) for the setup. The results in Fig. 3(c) show that the fiber transmission does not reduce the interference visibility, and hence the difference between the measured visibility and the calibration value can be utilized as the indicator of the intercept-resend attack.

C. Security of QSGI

The security of QSGI is based on that the R_{SN} of Eve's image is lower than that of Bob's. By controlling the data size of photon records Alice sends to Bob, Eve's R_{SN} is limited to be not higher than the recognition criterion. The data size is denoted as t, which is the measurement time of photon records sent by Alice. To show the difference between R_{SN}'s of Bob and Eve's images, first the image at Bob is constructed by quantum temporal ghost imaging under different t ($t \leqslant 20$ s, since Alice and Bob perform the detection for 20 s in each step). The R_{SN}'s of these images are calculated and shown in Fig. 4 (see the Appendix for details). The measured values are fitted by $R_{SN} = A\sqrt{t}$ and the experimental parameter A

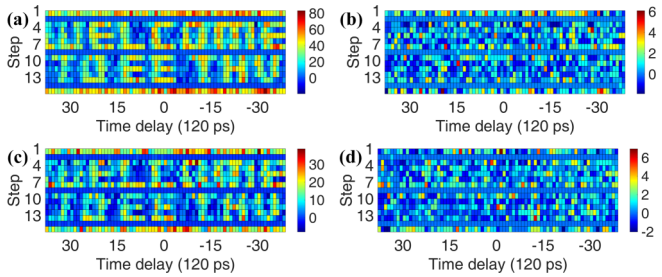

FIG. 5. Images constructed by Bob and Eve under intercept-resend eavesdropping. (a) and (b) are Bob's and Eve's images, respectively, when Alice confirms $\Delta V = 2\%$ and controls the data size sent to Bob. (c) and (d) are Bob's and Eve's images, respectively, for $\Delta V = 5\%$.

is calculated according to Eq. (2). By inspecting the image quality under different t, the recognition criterion is determined as shown by the dash line with $R_{SN} = 0.48$ under $t = 0.2$ s according to the fitting curve, and the inset shows the corresponding ghost image.

According to the analysis of the security test, if Eve perturbs the quantum channel by intercept-resend strategy, the intercept-resend fraction x can be obtained by the measured degradation of energy-time entanglement (ΔV). If the R_{SN} of the image at Eve is limited by the recognition criterion, the data size sent by Alice for ghost imaging can be calculated according to Eqs. (2) and (3) with the criterion defined in Fig. 4. Furthermore, Fig. 5 displays two cases under different ΔV introduced by Eve. In the first one the fringe visibility degrades by 2% ($\Delta V = 2\%$). Since the original visibility $V_0 = 86.4\%$ in the experiment, the eavesdropping fraction $x = 2.31\%$ according to Eq. (1). Hence, $t \leqslant 8.64$ for the security in the imaging process. By the coincidence measurement with Alice's photon records of 8.64 s, Bob and Eve can retrieve the image by temporal ghost imaging, which are displayed in Figs. 5(a) and 5(b), respectively. It can be seen that Bob's image is well recognizable ($R_{SN\,\mathrm{Bob}} = 3.16$), while Eve's image is blurry with the R_{SN} close to the criterion ($R_{SN\,\mathrm{Eve}} = 0.47$). Furthermore, if the degradation of the interference visibility increases to 5%, it can be calculated that $t \leqslant 3.4$ s. In this case, Bob's and Eve's images are displayed in Figs. 5(c) and 5(d), respectively. It can be seen that Bob's image is recognizable although the quality degrades with a smaller R_{SN} ($R_{SN\,\mathrm{Bob}} = 2.09$) compared to the previous case. Meanwhile, Eve's image is still blurry and unrecognizable ($R_{SN\,\mathrm{Eve}} = 0.40$). These results show that the R_{SN} of Eve's image could be controlled by the photon records Alice sends to Bob, demonstrating the feasibility of QSGI and protecting the process of ghost imaging between distant parties under the intercept-resend attack.

IV. CONCLUSION

To conclude, we propose and experimentally demonstrate the scheme of QSGI, which combines a quantum temporal ghost imaging and security test based on quantum entanglement over 50 km of commercial optical fibers between imaging parties. Entangled photon pairs are randomly directed to realize ghost imaging and security test in QSGI. In ghost imaging, spectrum patterns are imaged by the time-domain coincidence measurement of Alice's signal photons through the programmable filter and Bob's idler photons through the transmission fibers. Meanwhile, the security test is performed by the biphoton interference of broadband energy-time entangled photon pairs, and nonlocal dispersion cancellation is applied to avoid the broadening of the coincidence peaks due to the large dispersion of the fiber link. The security of QSGI is demonstrated by comparing the R_{SN}'s of images constructed by Bob and Eve in the temporal ghost imaging process under the assumption of Eve's intercept-resend attack over quantum channel. It shows that by controlling the data size of photon records Alice sends to Bob for ghost imaging, the quality of Eve's image can be limited to be unrecognizable, while Bob can succeed to image the patterns. The QSGI scheme could be applied in the scenario of secure imaging and surveillance and may inspire new ideas in specific quantum communication tasks.

ACKNOWLEDGMENTS

This work was supported by the National Key R&D Program of China under Contract No. 2017YFA0303704; National Natural Science Foundation of China under Contracts No. 61575102, No. 91750206, and No. 61621064; and the Tsinghua National Laboratory for Information Science and Technology.

APPENDIX: R_{SN} ANALYSIS

According to the protocol, since Alice only sends her records in the time bins declared by Bob, these records are useless for Eve if he simply intercepts some photons over the quantum channel. Hence, the intercept-resend strategy is reasonable for Eve. However, due to the quantum no-cloning theorem, the intercept-resend attack the intercept-resend attack degrades the quantum entanglement of photon pairs and can be checked by the security test. In our protocol, the biphoton interference of the energy-time entanglement is utilized for the security test.

Assuming that under the trusted condition excluding any eavesdropper's intrusion, the fringe visibility of the biphoton interference is V_0, which can be measured in system calibration and can be expressed as

$$V_0 = \frac{R_{\max} - R_{\min}}{R_{\max} + R_{\min}}, \tag{A1}$$

where $R_{\max}$ ($R_{\min}$) is the maximum (minimum) coincidence rate in the fringe. $R_{\min}$ is mainly due to accidental coincidences of noise photons in the system and dark counts of single photon detectors. In this case, the contribution of entangled photon pairs to the coincidence is $R = R_{\max} - R_{\min}$.

Supposing there is an eavesdropper (Eve) intercepting a fraction, denoted by x, of idler photons over quantum channel and resending the fake ones to Bob, $R_{\max}$ would decrease by $xR/2$ and Rmin would increase by $xR/2$, i.e.,

$$\begin{aligned} R'_{\max} &= R_{\max} - xR/2, \\ R'_{\min} &= R_{\min} + xR/2. \end{aligned} \tag{A2}$$

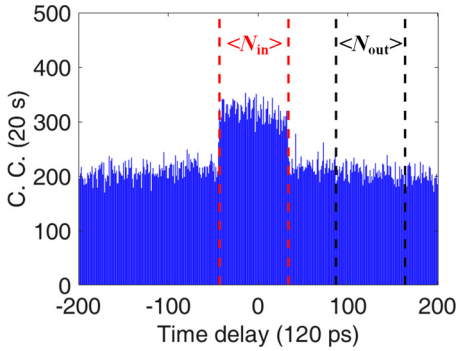

FIG. 6. The raw coincidence histogram of the first line of ghost imaging in Fig. 3(b). C. C., coincidence count.

The ratio of 1/2 is due that the fake idler photons (xR) would randomly exit from the two output ports of the interferometer. As a result, the fringe visibility would be

$$V = \frac{R'_{\max} - R'_{\min}}{R'_{\max} + R'_{\min}} = \frac{R_{\max} - R_{\min} - xR}{R_{\max} + R_{\min}} = V_0(1-x), \tag{A3}$$

and therefore, the degradation (ΔV) is

$$\Delta V = xV_0. \tag{A4}$$

Hence, if the entanglement degradation is measured in the security test, the fraction of intercept-resend photons can be calculated.

On the other hand, the quality of the image constructed by quantum temporal ghost imaging could be indicated by its signal-to-noise ratio (R_{SN}) [30,31]. Theoretical analysis shows that if the object is a mask with binary transmission levels (the transmission $T = 0$ or 1 at each pixel), R_{SN} can be defined as [31]

$$R_{SN} \equiv \frac{|\langle N_{\text{in}} - N_{\text{out}}\rangle|}{\sqrt{\langle \delta^2(N_{\text{in}} - N_{\text{out}})\rangle}}, \tag{A5}$$

where N_{in} (N_{out}) is the coincidence count inside (outside) of the object pattern, corresponding to $T = 1$ (0). For quantum ghost imaging the coincidence events at different pixels are independent and satisfy the Poisson distribution, R_{SN} can be simplified as [30]

$$R_{SN} = \frac{|\langle N_{\text{in}}\rangle - \langle N_{\text{in}}\rangle|}{\sqrt{\langle N_{\text{in}}\rangle + \langle N_{\text{out}}\rangle}}. \tag{A6}$$

In the experiment, the raw coincidence histograms of the first and last lines in the image are used to calculate the R_{SN}. Figure 6 shows the raw histogram of the first line in Fig. 3(b). The region between the two red dashed lines corresponds to the first line of the image, in which all the pixels are transmitted, and hence all the signal photons in the frequency region of 1544–1558 nm can pass through the programmable optical filter. The coincidence counts in these pixels of the first and last lines are averaged as $\langle N_{\text{in}}\rangle$. On the other hand, the coincidence counts outside this region are accidental coincidence counts, which are in the same level of the coincidence counts in pixels where signal photons with specific wavelengths are blocked by the programmable filter. Therefore, the accidental coincidence counts in the first and last lines are averaged as $\langle N_{\text{out}}\rangle$.

The difference of $\langle N_{\text{in}}\rangle$ and $\langle N_{\text{out}}\rangle$ can be expressed by the generation rate of photon pairs R and the measurement time of the single photon detection t:

$$\begin{aligned} \langle N_{\text{in}}\rangle - \langle N_{\text{out}}\rangle &= R\eta_{\text{A}}\eta_{\text{B}}/k, \\ \langle N_{\text{in}}\rangle/\langle N_{\text{out}}\rangle &= \xi_{\text{CAR}}. \end{aligned} \tag{A7}$$

where η_{A} (η_{B}) is the collection efficiency of signal (idler) photons for ghost imaging at Alice (Bob), and k is the horizontal pixel number of the image. ξ_{CAR} is the ratio of coincidence count to accidental coincidence count. Hence, R_{SN} of Bob's image can be calculated as

$$R_{SN\,\text{Bob}} = \sqrt{\frac{\xi_{\text{CAR}} - 1}{\xi_{\text{CAR}} + 1}\frac{R\eta_{\text{A}}\eta_{\text{B}}}{k}t}. \tag{A8}$$

Obviously, it is proportional to the square root of the measurement time t.

If Eve's intercept-resend fraction is x, the ratio of Eve's (accidental) coincidence counts and Bob's (accidental) coincidence counts is also x after Alice and Bob perform the bin sifting with each other by the classical channel. Hence, the relation between R_{SN}s of images at Bob and Eve is

$$R_{SN\,\text{Eve}} = \sqrt{x}\, R_{SN\,\text{Bob}}. \tag{A9}$$

It can be expected that Alice can control the R_{SN} of the image at Eve and make it not higher than the recognition criterion by limiting the data size Alice sends to Bob through the classical channel. It prevents Eve from obtaining the object information from his eavesdropping. On the other hand, the data size should be large enough to make the R_{SN} of Bob's image higher than the criterion, realizing the ghost imaging between Alice and Bob. In detail, supposing the R_{SN} criterion of the specific set of patterns is denoted by C and Eve cannot recognize the patterns if the R_{SN} of his image is

$$R_{SN\,\text{Eve}} \leqslant C. \tag{A10}$$

According to Eqs. (A4), (A8), (A9), and (A10), if t satisfies

$$t \leqslant C^2\frac{V_0}{\Delta V}\frac{\xi_{\text{CAR}} + 1}{\xi_{\text{CAR}} - 1}\frac{k}{R\eta_{\text{A}}\eta_{\text{B}}}, \tag{A11}$$

Bob can construct a recognizable image, while Eve fails to image the object with the intercept-resend eavesdropping.

[1] Y. H. Shih, IEEE J. Sel. Top. Quantum Electron. **13**, 1016 (2007).
[2] T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, Phys. Rev. A **52**, R3429 (1995).
[3] A. Valencia, G. Scarcelli, M. D'Angelo, and Y. H. Shih, Phys. Rev. Lett. **94**, 063601 (2005).
[4] J. H. Shapiro, Phys. Rev. A **78**, 061802 (2008).
[5] O. Katz, Y. Bromberg, and Y. Silberberg, Appl. Phys. Lett. **95**, 131110 (2009).
[6] B. I. Erkmen and J. H. Shapiro, Adv. Opt. Photonics **2**, 405 (2010).

[7] P. Ryczkowski, M. Barbier, A. T. Friberg, J. M. Dudley, and G. Genty, Nat. Photonics **10**, 167 (2016).
[8] F. Devaux, P. A. Moreau, S. Denis, and E. Lantz, Optica **3**, 698 (2016).
[9] S. Dong, W. Zhang, Y. D. Huang, and J. D. Peng, Sci. Rep. **6**, 26022 (2016).
[10] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, Opt. Lett. **35**, 2391 (2010).
[11] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, Appl. Phys. Lett. **101**, 101108 (2012).
[12] W. Chen and X. D. Chen, Appl. Phys. Lett. **103**, 221106 (2013).
[13] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
[14] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).
[15] J. Y. Wang *et al.*, Nat. Photonics **7**, 387 (2013).
[16] J. Yin *et al.*, Science **356**, 1140 (2017).
[17] S. K. Liao *et al.*, Phys. Rev. Lett. **120**, 030501 (2018).
[18] G. L. Roberts *et al.*, Nat. Commun. **8**, 1098 (2017).
[19] H. L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **95**, 032334 (2017).
[20] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nat. Commun. **5**, 3717 (2014).
[21] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, Npj Quantum Information **3**, 7 (2017).
[22] J. Y. Guan, J. M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang, and J. W. Pan, Phys. Rev. A **97**, 032338 (2018).
[23] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, Nature **501**, 69 (2013).
[24] Y. Fu, H. L. Yin, T. Y. Chen, and Z. B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).
[25] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, Appl. Phys. Lett. **101**, 241103 (2012).
[26] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
[27] T. Zhong *et al.*, New J. Phys. **17**, 022002 (2015).
[28] P. R. Tapster, J. G. Rarity, and P. C. M. Owens, Phys. Rev. Lett. **73**, 1923 (1994).
[29] S. Rogers, D. Mulkey, X. Y. Lu, W. C. Jiang, and Q. Lin, ACS Photonics **3**, 1754 (2016).
[30] M. N. O'Sullivan, K. W. C. Chan, and R. W. Boyd, Phys. Rev. A **82**, 053803 (2010).
[31] G. Brida, M. V. Chekhova, G. A. Fornaro, M. Genovese, E. D. Lopaeva, and I. R. Berchera, Phys. Rev. A **83**, 063807 (2011).
[32] W. J. Zhang *et al.*, Sci. China: Phys., Mech. Astron. **60**, 120314 (2017).
[33] J. D. Franson, Phys. Rev. A **45**, 3126 (1992).
[34] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, Phys. Rev. A **90**, 062331 (2014).